A Chain Perspective on Large-scale Number Systems

J. (Jan) H.A.M. Grijpink
Emeritus Professor,
Utrecht University, The Netherlands
j.h.a.m.grijpink@uu.nl

As large-scale number systems gain significance in social and economic life (electronic communication, remote electronic verification), the correct functioning and the integrity of public number systems take on crucial importance. They are needed to uniquely identify people, objects or phenomena. Number systems are deeply embedded in our society. They fulfil many functions, often several at the same time. Due to poor system design and management people can in many ways manipulate number systems or number verifications to commit identity fraud. Moreover, personal numbers are often used as 'proof' of identity both online and offline. At present, our large-scale number systems are vulnerable to the misuse of personal numbers (identity fraud/theft). The usual multi-chain usage of personal number systems at the national and the European level proves to be very problematic.

The quality of the design and the management of number systems is becoming more and more vital to our information society. Unfortunately, large-scale number systems have long been neglected in Public Administration and Information Science. Therefore, this article presents a number system theory based on the theory of Chain-computerisation. It explaines some important insights that have to be taken into account when designing, implementing and managing large-scale number systems.

Keywords: personal number, large-scale number system, Chain-computerisation, information strategy, identity fraud/theft, interoperability, privacy, security, safety

1 Introduction

Decisions about large-scale number systems are of great importance to our emerging information society, because number systems are needed to register and exchange information about people, objects or phenomena. Unfortunately, the large-scale application of number systems has long been neglected in Public Administration and Information Science. Yet, politicians, public administrators and information professionals are confronted with difficult strategic choices regarding design, implementation and management of number systems. Choices must be made between a general number and a set of several independent (chain) numbers; adopting an existing personal number for a new purpose and introducing a new tailor-made personal number (Grijpink, 2002b); a personalised number, a pseudonym and an entirely anonymous number (Grijpink & Prins, 2003); an interoperable number system that can accommodate numbers from other similar number systems and a non-interoperable number system (Hayat, Posch & Rössler, 2005); a public and a private number system. Shortcomings in design and implementation of large-scale systems are difficult or impossible to remedy afterwards.

Therefore, this article presents theory of number systems based on the theory of Chain-computerisation (Grijpink, 1997, 2000a, 2000b). It builds on prior publications on number systems, identity fraud and biometrics (Grijpink, 2002b, 2004, 2008). It explaines some important insights that have to be taken into account when designing, implementing and managing large-scale number systems. This article especially focuses on personal number systems but insights that apply to personal numbers are often applicable to other numbers. Once we stop considering number systems as unimportant administrative or technical details, we will gain a clearer view of the difficult choices that number systems present in the political, administrative and management areas.

Section 1 introduces some core concepts: number system, number system application, identity, identity fraud, chain perspective on number systems and number strategies. The following sections 2-4 elaborate on some important properties and legal aspects of number systems and explain more fully the various possible types of number strategies with their pros and cons. Section 5 presents a checklist for a more robust design, implementation and management of large-scale number systems.

1.1 Number system and number system application

Number systems are logical series of numbers that are used to identify persons, objects and phenomena within a defined or definable group. A number can also be used as a key to retrieve related data from databases. Numbers can be numerical (purely digits) or alphanumerical (digits and letters).

The term 'system' is taken to mean that the number is assigned and later withdrawn according to certain rules, and that the use of the number is subjected to certain rules, as well. Table 1 shows some examples of number systems.

Table 1. Examples of number systems

1	serial number at the butcher's
2	postal code + house number
3	car registration number
4	document number (e.g. passport number)
5	road number
5	telephone number
6	Internet address (IP address)
7	client number
8	bank account number
9	citizen service number (Burgerservicenummer, BSN)

In this article the concept of 'number system application' is used to indicate that any number system can be considered being implemented within a larger context that can be characterised by a number of dimensions such as geographic area, domain, purpose or degree of voluntary use.

1.2 Identity management and number systems

The increasing use of numbers is a phenomenon that is inherent in the advancing computerisation of our society. Numbers are increasingly used in electronic data processing. In practice, a personal number is even used as a 'proof of identity', both online and offline, both honestly and dishonestly. Rightly or wrongly, numbers enable claiming rights or other advantages and facilitate rendering oneself invisible and untraceable by hiding behind somebody else's personal number.

This dual use of numbers is also revealing the vulnerability of number systems if not properly designed, implemented and managed. It turns out that there are many ways to frustrate number verifications, and identity fraud using personal numbers is rising sharply. At present, the attention paid to the misuse of personal numbers mainly focuses on breaches of privacy, but that should be extended more and more to security breaches. A compromised personal number can result in the victim having to spend years defending himself against a wrongful suspicion or conviction, followed by a bitter struggle to restore his reputation or recover his loss. Often in vain, for the victim is initially taken as the perpetrator (after all, the victim's personal number has been used!), and is often unable to prove his innocence. This underlines that privacy and security are becoming increasingly intertwined. Therefore, in our privacy debates, we should direct our attention more and more towards regulating the use of identities in general and preventing identity fraud as important privacy enhancing security aspects of large-scale number systems.

1.3 The chain perspective on number systems

A chain can be seen as a temporary pattern of interorganisational co-operation triggered by a dominant chain problem that no chain partner can solve alone. That problem can differ between chains. To prevent a chain from being disrupted by systematically failing to deliver its social product (health, security, prosperity) this dominant chain problem calls for a structural partnership. This is not easy, because there is no all-encompassing authority in a chain, as a result of which chain-wide decision-making processes are unclear and rather irrational (Grijpink, 1997, pp. 131-144; 2002a, pp. 19-31; 2010b, pp. 27-36). In this barely manageable environment, a dominant chain problem creates an interplay of forces more inviting to co-operate than any other type of interorganisational problem in a chain. If this dominant chain problem cannot be solved without using a chain number system, this dominant chain problem determines the requirements for its design, implementation and management.

Only when the number system is absolutely indispensable to solving the dominant chain problem, it can maintain itself at chain level for a longer period of time, because there will be sufficient support for a common management of the number system in accordance with the requirements set by that specific dominant chain problem. The shorter the distance between a number system and its dominant chain problem the more its management can benefit from chain-related self-cleaning and self-resolving mechanisms. Because of the grip of the dominant chain problem on a chain number system, its chain-wide support is much greater than that for a number system that has no direct relationship with a dominant chain problem.

1.4 Number strategies

With the concept 'number strategy' we mean the dynamic complex pattern of general and chain number systems resulting from government measures and behaviour of number users and number system managers. This concept can be illustrated with the example of the Dutch number strategy.

> Example **The Dutch number strategy**
> For decennia the Dutch residents were registered using a confidential administration (A-) number and a confidential fiscal (FI-) number. The A-number has been kept confidential, but since 1985 the FI-number has been regarded as a public number which was introduced in the social security sector in 1988: the Dutch SOFI-number came into being. In 2001 the Dutch legislator decided that this SOFI-number could serve as an education number, as well. In 2007 the SOFI-number was renamed Citizen Service Number (Burgerservicenummer, BSN) by law and assigned the role of general personal number to be compulsorily used by all government agencies. In June 2008, the BSN was also introduced in the public-private health care sector to be compulsorily used for storing and exchanging medical data. This emerging Dutch number strategy is moving towards a mandatory general personal number system, which - because of this compulsory use – will gradually oust existing chain number systems and prevent new ones from being introduced.
>
> Then the behaviour of number managers and number users must be taken into account. After the introduction of the then SOFI-number in the social security area in 1985 identity fraud increased sharply. Nowadays, many people have been wrongly issued more than one BSN; others make use of someone else's BSN and identity, with or without the consent of the rightful holder. This way, the BSN number system is gradually corrupting inportant public registries, e.g. criminal and medical records. The emergence of the Dutch number strategy was not checked by these problematic behavioural effects.

This example of the Dutch SOFI/BSN number system shows what can happen with any number system unless its design, implementation and management guarantees that the numbers are being sufficiently guarded and protected against misuse after being issued. If this is in fact possible depends on the type of number strategy in place.

As number systems gain significance in social and economic life (electronic communication, remote electronic verification), the correct functioning and the integrity of public number systems take on crucial importance. But large-scale number systems, especially mandatory general public personal number systems, are difficult to manage without additional personal data. That is why - next to a general number system - a few chain number systems with related personal data are indispensable as the independent suppliers of verifying details. It is the prevailing national number strategy that makes this possible, or not.

2 Properties of number systems

Five properties of number systems are discussed in this section: (1) the function, (2) the scope of the number system's application, (3) unicity, (4) number format and (5) number semantics. Combinations of properties result in specific applications with pros and cons offering a great diversity of possible solutions to those designing, implementing or managing a number system.

2.1 Function

Number systems fulfil many functions, often several at the same time. The ability to uniquely identify a single instance in a series is in itself an important function. A case in point is when one wishes to lay down a detail in a register or indicate a certain sequential order, as a butcher would, for instance. By using a number it is possible to trace a detail and also establish that two details are

related, for verification purposes, for instance. When comparing details of the same persons, objects or occurrences from various sources, linking by number can prevent or, conversely, reveal errors. Verification is often more accurate with numbers than only with words (name and address details) or images (photograph, signature, logo). Take into account that foreign names can be written in different ways and that certain names can be very common.

If a number contains a property of a person or object, this information can easily be passed on to somebody else by using the number (e.g. year of birth, sex, expiry or place of issue). Random numbers, conversely, can protect against this implicit information transfer.

Number systems improve the management of data collections by counteracting contamination and fraud with other numbers and related details. It is important in this context that number systems not only facilitate verifying an individual detail, but also - at the level of the number series as a whole - detecting any double occurrence or number omission. It is important, for instance, to the quality of a personal number system to be able to check whether somebody is wrongly using several unique personal numbers or that a unique personal number is wrongly being used by several people.

2.2 Scope of the number system's application

Number systems have a certain scope of application, regarding both content and geographical range. The butcher's serial number is used for serving customers (the content aspect) locally in the shop (the geographical aspect). Other number systems are public and are used in a sectoral or chain context. A car registration number relates to cars and road traffic in all its aspects (content) and can, depending on the country of registration, be used by everybody, both nationally and internationally (the geographical range). Besides sectoral or chain numbers, there are also inter-sectoral or multi-chain number systems. These numbers are used in more than one sectors or chains. Finally, there are general national numbers. Viewed from the perspective of the Netherlands, this is the most extensive area of application, but from an international perspective a number of this nature is also geographically and functionally limited in more or less the same way as sector and chain numbers. The use of these national numbers does not have to be the same within the entire geographical area of application. In the one region a sector can use its own sectoral number, for example, while the same sector in another region uses the general national number.

Running ahead of our later analysis in subsection 4.2, it is interesting to mention here the gradual changes in the scope of application of the Dutch SOFI-number/BSN as explained in subsection 1.4. Within twenty years, the SOFI-number developed from an internal, confidential personal number towards a national general personal number with compulsory usage in the public and the private domain.

2.3 Unicity

A number's unicity has at least two dimensions: place and time.

A house number is permanently unique within the geographical limitation of the street. It is not related to one particular house, as once that house has been demolished it will be reassigned to a new one at the same location. Missing house numbers are not important, because they do not affect the house's unique identity or the courrier being accurately delivered.

The serial number at the butcher's is an example of a unique local number that has a very short life-span. This number can be disposed of immediately after use. Important is only that two identical numbers do not occur at the same time in the queue. Missing numbers or series of numbers are not important, because they do not affect the order of the numbers that are present.

Other numbers are temporarily unique for a longer period of time in a large geographical area. A car's chassis number, for example, must remain unique for a long period of time and requires a large geographical range. That number does not lose its significance until the car is scrapped. After a certain waiting period, the number could be re-assigned. A temporary unique number is also sufficient in the area of immigration and naturalisation. The so-called alien number must guarantee for the period of time that a refugee stays in the Netherlands seeking asylum that data and decisions relate to the right person. Ultimately, however, that person is granted the Dutch nationality or is forced to leave the country. The alien number can then be thrown away. If the number is to be retained for longer in order to prevent a rejected asylum seeker re-applying for asylum, it is better to rely on a fingerprint check than a number.

Conversely, a BSN must last for longer than a person's life since confusion with the data of somebody else must be avoided for many years after a person's death. What is required for this is a unique number which is only re-assigned to another person after e.g. 150 years.

2.4 Number format

Number systems feature a wide range of formats. A telephone number in the Netherlands has ten positions, a BSN/SOFI-number nine. The number of positions required depends on the application. A number does not have to contain only digits, but can also hold letters. An apartment, for example, is often indicated with a combination of digits and a letter. Car registration numbers and chassis numbers in many countries are also alphanumeric. One of the advantages of letters in a number is that a position of a letter can have 26 different values, as opposed to that of a digit which only offers ten alternatives (0-9). Another advantage is that a number containing digits and letters is usually easier to read and to remember than a number of equal length containing only digits.

2.5 Number semantics

Numbers often contain visible or hidden information (Blocksma & Van Maanen, 1990).

Many personal numbers make use of the date or year of birth, thus indicating the holder's age.

Those who know that the road network in the Netherlands is numbered clockwise from Amsterdam can use this concealed information without much topographical knowledge to work out that the A1 directly connects to Amsterdam, whereas the A27 does not.

The German car registration number indicates with the first letters the area in which the car is registered. The Dutch car registration number, on the other hand, contains a sequential national number system with six letters and digits, so that the number individually indicates the approximate year in which the registration number was issued.

Some numbers also contain a control digit to check whether there is anything wrong with the number. The BSN/SOFI-number, for instance, consists of 9 digits, the last of which is a control digit. To calculate that last digit, the first digit is multiplied by 9, the second by 8, and so on until the eighth digit which is multiplied by 2. The results of these eight multiplications are added together and divided by 11. The digit that is carried after the division forms the ninth digit of the BSN. This control digit makes it possible to detect writing errors or numbers that cannot exist (Blocksma & Van Maanen, 1990, p. 87).

3 Legal aspects of number systems

This section discusses the legal position of a number system from the perspective of the European Data Protection Directive. Number systems for legal entities, immovable property, objects, locations or transactions are not subject to special data protection rules unless they qualify as personal data. Data protection of personal data has been harmonised within the European Union, Directive 95/46/EC. Keep in mind that there are often special laws applicable, too, such as - in The Netherlands - the Passports Act (e.g. in relation to the document number) or the Municipal Administration Act (GBA), for the A-number used in that Act. Together, these govern the use of any number that can be traced to a person with reasonable effort. In that case the lawful use of the number is subject to many conditions, with additional conditions if the personal number with its related data is legally defined as *sensitive* personal data.

To establish whether a number is a personal detail one should view the application as a whole rather than looking only at the number itself. We therefore have to take account of all the surrounding technical, procedural and organisational provisions. A person whose identity cannot be established without making a disproportionate effort is considered anonymous. If a personal number is kept anonymous within an application, no special protection or provisions for its use are required. Semi-anonymity (also called pseudonymity) is defined as there being at least one body that knows (e.g. the body that issued the number) the identity of the personal number holder, while other users of the personal number cannot find out.

Given below is a privacy law based policy framework for personal numbers or other numbers that in terms of data protection must be regarded in a specific application as personal data. The eight aspects discussed are: (1) purpose and purpose-restricted data-processing, (2) proportionality and subsidiarity, (3) delimitation of the target group, (4) voluntariness, (5) scale of application, (6) central versus decentral storage of the numbers, (7) **s**hielding and encryption of personal numbers and (8) independent supervision.

3.1 Purpose and purpose-restricted data-processing

The purpose of using personal numbers must be clear and known to all parties involved. The re-

quirement of clarity and knowledge is in principle met in the case of use by (semi) public authorities if usage is provided for in a generally binding regulation. It is not permissible to collect and/or use personal numbers in violation of the current regulations. In assessing the legitimacy of an application, the balance of power between citizens and government - or between clients and companies - plays an important role. There is, however, also a grey area in which it is less easy to establish whether the application is legitimate. It is in any event important that unrestricted purposes are to be avoided.

In principle, the use of a personal number should remain restricted to the original purpose of its registration. But the increase in identity fraud does however give rise to the question of whether processing control data to protect someone's identity against being stolen by another person, automatically makes this data-processing legitimate secondary use ('compatible processing') following the definition given by the Data Protection Directive, even if the control data were originally collected for a different purpose. Purpose-restriction remains a dynamic criterion. May number administrators mutually compare their personal details related to the same person as legitimate secondary use in order to detect identity fraud or to counteract the contamination of medical files with medical details of people other than the lawful holder of that citizen service number? The answer is probably yes if this is properly regulated and known to the person concerned. It is certainly yes if the person concerned has requested this protection himself.

3.2 Proportionality and subsidiarity

The use of a number system must be proportional, which means in reasonable proportion to the purpose for which it is used.

Subsidiarity means that if the objective can also be achieved in another, less radical way, that way must be given preference. The objective must for example justify the use of a personal number being compulsory; otherwise the number must be used voluntarily. Another example: a personal number should not be centrally stored if its objective can be equally well achieved with non-central storage on a chipcard in full control of the holder of the number. The subsidiarity requirement is also met by using a number with less far-reaching properties (such as a temporary number rather than a permanent one) or by using masked or truncated numbers in such a way that it is not possible to infringe someone's privacy or security. Compare the Austrian masking solution with that of the Dutch, see under subsection 3.8 or a truncated BSN 'xxxx3412x' (in the case of a BSN, the control digit should not be shown). The subsidiarity principle implies that a general personal number must not be stated in full on the identity card, because a copy of an identity card with the full number would make identity fraud too easy while most verification can also be done with a truncated number. After all, the rightful holder can reasonably be expected to state the correct, full personal number if he sees this truncated number on his identity card.

Despite all restrictions applicable to numbers registered by name, people generally opt for a personalised number system, even if the purpose of the application would be equally well served with anonymous or semi-anonymous numbers. Therefore, the subsidiarity principle provides some room for improvement of our large-scale number systems!

3.3 Delimitation of the target group

The number system's target group must be clearly defined. This is especially important to communication with that target group and to the way in which the relationship between the parties involved is legally formalised. If the target group comprises the entire population of the Netherlands or a municipality, it makes sense to regulate the number system by legislation or (municipal) by-law. If, on the other hand, the target group is the personnel of a company or a shop's clientele, it will be appropriate to include regulation in the collective labour agreement or employment contract or general terms and conditions, respectively. Finally, the precise delimitation of the target group is also important for auditing of the data collection.

3.4 Voluntariness

Leaving aside the moral and ethical limits and measures designed to protect people from themselves, the voluntary use of personal numbers for private purposes is in principle permitted. But when is voluntary co-operation truly voluntary? If a party occupies a monopoly position or a position of power, such as the government in relation to the citizen or the employer in relation to an employee, that co-operation cannot be regarded as completely voluntary. It is not however only these market conditions that determine the issue of true freedom of choice. Complete freedom of choice can only exist if there is an alternative of equal value without the compulsory use of the number.

A party who issues or uses a personal number will have to meet stricter conditions as the voluntary use of the number is less obvious. An example of such a condition is that the voluntary character must be attested to by the unequivocal, express permission of the personal number holder.

3.5 Scale of application

A large-scale general personal number is a likelier candidate for government supervision or regulation than a small-scale sectoral personal number. This is because of the security and privacy risks of a large-scale general personal number system being less controllable and the chances of successful identity fraud being greater. Small-scale applications are less risky and could in principle also promote security and privacy; certainly if there are many small scale applications with various, independently managed number systems.

3.6 Central versus decentral storage of the numbers

'Central' in this context means that all stored personal numbers with the additional personal details are directly accessible and can be compared in a single run. The data can be physically stored in one place, but that is not necessary. The two extremes considered here are storage in a central database of all numbers and non-central storage, where each number is stored separately on a document or chip card that is issued to the holder.

Using a central database in this sense makes it possible to carry out checks that would not otherwise be possible. A number administrator with a central database can for instance establish whether someone has already been included in the collection but under another number. He can also ascertain whether a number is registered in the name of more than one person (which is not the same as someone using someone else's personal number, which the number administrator cannot see).

The distinction between central and non-central is of legal significance because central storage involves more social risks. In the case of a specific application, the number issuing authority will have to compare the alternative solutions and find a reasonable balance between purpose and risks.

3.7 Shielding and encryption of personal numbers

The storage and use of personal numbers must be appropriately safeguarded, and the level of security must be higher in keeping with the interest involved in the personal number being protected. From the security point of view, unauthorised access to and/or use of personal numbers must therefore be prevented, and traditional security measures must be in place, including encryption. This security requirement of the Data Protection Act differs from the requirement that the Dutch Penal Code sets for a punishable violation: a violation is only punishable if 'any security' shows that there was a will to protect the number.

The shielding or encryption of a personal number deserves a special mention since there are new developments in this area that could have implications for large-scale personal number systems in the European Union. This concerns the Austrian model (Hayat, Posch & Rössler, 2005).

In this subsection 3.7 we look mainly at the shielding and encryption part of the Austrian model. This model has also been shown to facilitate the interoperable use of different national personal number systems, so that each EU country does not need to issue its own personal numbers to residents of other EU countries and thus ultimately saddling all EU residents with dozens of different national personal numbers. We will discuss this interoperability with other national personal number systems and the model's sector-specific derivation of disposable personal numbers, two other elements of the Austrian model, in subsections 4.1 and 4.2.

The Austrian model (PIN—sourcePIN—ssPIN)

In this model, the unique national personal identification number (PIN) is prevented from being taken outside of the central population register. Instead, the central authority first issues each citizen with a pseudo-personal number derived from that PIN, which is labelled 'sourcePIN'. This sourcePIN is obtained by adding a secret value to the secret PIN and encrypting the resulting number with the secret key of the central sourcePIN authority. This sourcePIN is only issued to the holder in combination with the public key of the issuing central sourcePIN authority, on a token the holder of the sourcePIN can use to place his electronic signature. The sourcePIN itself may not be used; even the issuing central sourcePIN authority is not permitted to keep a copy of it.

If the decryption using the public key of the central sourcePIN authority yields a readable certificate, we know that the holder of the token is the right person and we also know for sure that the (hidden) sourcePIN is authentic, even though it is not possible to get hold of the sourcePIN itself.

For each public sector a separate, sector-specific PIN (ssPIN) is then derived from the sourcePIN by adding the sector code to the sourcePIN and then applying a one-way hash function that ensures that neither the sourcePIN nor another ssPIN can be derived from an ssPIN. Therefore, sector-specific personal numbers belonging to the same citizen cannot be traced back to each other, either. This facilitates protected sector-specific online communication with and about the citizen, as well as administrative verification and data linkage (Hayat et al., 2005).

This protection of the original PIN and the sourcePIN derived from it is a technical safeguard at the level of the personal number itself, a welcome addition to the current security measures at higher system levels, such as the personal number system as a whole (e.g. a password-protected token), the procedure (e.g. authorisation) and the organisation (e.g. job separation).

The general idea underlying the shielding and encryption of personal numbers is that in the event of loss, theft or other misuse it is possible to derive new sector-specific PINs as required, without placing the original PIN or the sourcePIN under threat. For that reason, we refer to these sector-specific PINs as disposable personal numbers.

3.8 Independent supervision

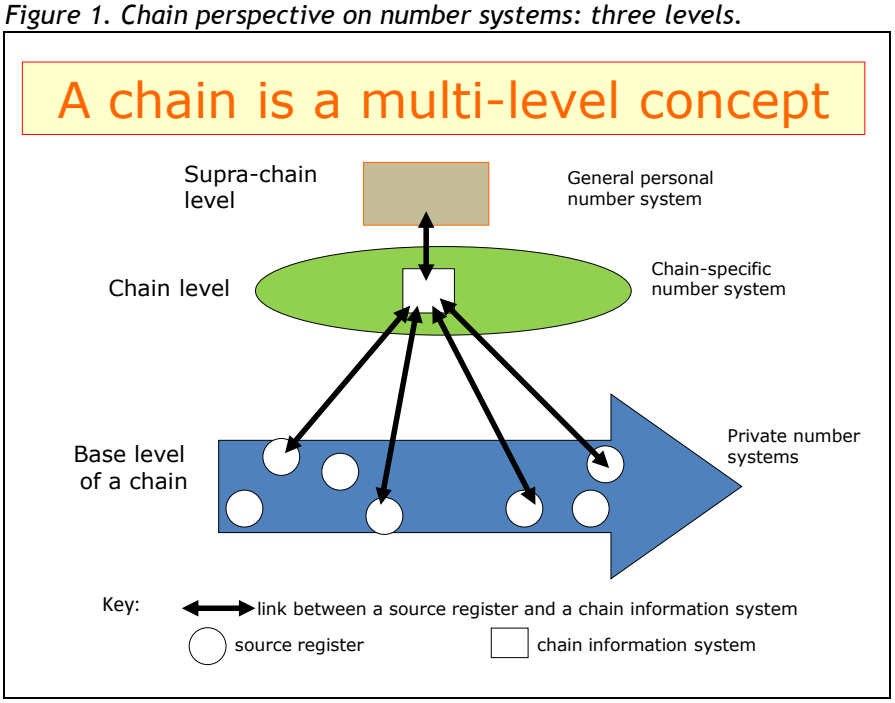
It can be desirable to have the management and the use of personal numbers supervised by an independent party. This could be the Data Protection Authority or the so-called privacy-officer provided for in the Data Protection Law. Other options include an ombudsman or a trusted third party.

4 Number strategy

This section presents a number of strategic starting points for how a number system should be positioned and managed. We discuss seven subjects related to number strategies: (1) positioning (vertical and horizontal), (2) chain linkage: the impact of a dominant chain problem, (3) multiple-chain usage of a number system, (4) number system management, (5) social effects of number systems, (6) Type of number strategy: single, multiple or composite, (7) development patterns of number systems.

4.1 Positioning (vertical and horizontal)

Figure 1. Chain perspective on number systems: three levels.



4.1.1 Vertical positioning: at chain level, below or above

Figure 1 shows how number systems can be positioned *vertically* at three levels: (1) internal private number systems at the base level of a chain, (2) chain number systems at chain level and (3) general number systems at supra-chain level.

A number system at the base level of a chain refers to an organisation that manages its own private number system. These internal number systems are used by one or more parties in the chain in their direct communication from their own source registers.

If the system is managed collectively by or on behalf of all organisations in the chain, i.e. independently of the individual chain partners' interests, a number system can be seen as positioned at chain level. A so-called chain number system is part of the information infrastructure of a chain (Grijpink, 1997, pp. 89-109; 1999, pp. 33-35) supporting and steering information exchange in the chain from the chain level.

General number systems can be found at a level above chains. These are not chain-based and can be used for many applications in many chains, national and international, depending on specific arrangements.

4.1.2 Horizontal positioning: interoperability

That takes us to horizontal positioning: what should we do about similar numbers from other domains or countries? This strategic choice is important to the future of many national and chain-specific personal number systems in the European Union, whether it concerns the medical dossier, the criminal record or any other socially important area of European chain co-operation.

Will residents of other EU Member States in the Netherlands be given a Dutch BSN for their relationships with the Dutch government, or will we opt for a system in which non-Dutch numbers can be incorporated? In that case we could describe the system as being interoperable, as experimentally demonstrated for the Austrian model (Hayat et al., 2005) by applying the PIN—sourcePIN—ssPIN transformation and their procedures to any foreign personal number (see subsection 3.7). Will a foreign patient be given a unique Dutch citizen service number, or will we opt for interoperability?

In the current situation, the Netherlands is opting for a non-interoperable system in which all foreigners with a relationship with the Dutch government will be assigned a unique Dutch BSN. That way, the stock of available national numbers will be exhausted at a faster rate and European citizens will eventually be burdened with a number of unique national personal numbers from any of the 27 EU-member states. Not to mention the multitude of other countries' sector or chain numbers.

The positioning of number systems is of strategic importance to the quality of life within the European Union, because as the European integration is progressing the number of different, non-related personal numbers for an average European citizen will grow tremendously.

4.2 Chain linkage: the impact of a dominant chain problem

A number system must be designed, implemented and managed primarily for its function in the chain with focus on the dominant chain problem. In a barely manageable large-scale environment such as a chain, particularly a dominant chain problem can trigger interorganisational co-operation (subsection 1.3). For as long as a personal number system is absolutely necessary to the chain-wide co-operation to tackle the dominant chain problem, there will be sufficient support for a common management of the number system in accordance with the requirements of that specific dominant chain problem. If an existing chain number is no longer as necessary as it was, the chain partners are no longer motivated to properly manage the chain number system and actively monitor it against misuse and fraud. The contamination of the number system and related registers increases, and - ultimately – the number system will be only occasionally used internally by a few chain partners. In terms of the theory of *Chain-computerisation*, that number system then loses its chain position and ends up at the base level of the chain. A realistic chain concept such as this is useful to understanding the difficulties and vicissitudes of number systems in chains.

Non-chain-related numbers (both internal and public general) are in principle more difficult to manage. The starting point for a number strategy is therefore that the number system is chain-related. Chain linkage can however be achieved in various ways, with the extreme variant being a number system that may or cannot be used outside of a specific chain.

Two other forms include the chain-specific derivation of ssPINs from the secret sourcePIN as described in 3.7 (Hayat et al., 2005) or a chain-specific linking of a general personal number to a

(any) chain-related personal detail. In the latter case, the Dutch citizen service number, for instance, could still be used in the healthcare sector, but only extended with several positions for an unvarying personal characteristic that is easy to check for authorised professionals (blood group and rhesus factor, for example) or a chain-specific detail that cannot otherwise be easily found out by an outsider. The advantage of this chain linkage is that only the BSN is given in the identity card, while the additional positions correspond with medical details that are regularly and carefully checked as a matter of course during the medical treatment, without that being considered an identity check! That way, someone's personal details can be more safely linked within a chain than with the citizen service number alone, while personal details of the same person from another chain cannot be directly linked.

Finally, chain linkage proves to be a good starting point for all personal number systems due to the European Data Protection Directive. This requires for all processing of personal details that this is done with the same objective as the data are originally gathered. If it is indispensable to tackling a chain's dominant chain problem, a personal number system meets at chain level the requirements of legitimate personal data processing.

Because chain linkage is crucial in many chains, chain linkage is a good starting point for all personal number systems, and an important factor when considering or assessing a number strategy.

4.3 Multiple-chain usage of a number system

This point can best be explained with the example of the Dutch SOFI-number/BSN from subsection 1.4. Its gradual development of the citizen service number BSN from secret internal FI-number to compulsory general BSN and health care number is summarised in Table 2.

Table 2. Development of the SOFI-number/citizen service number BSN

Policy area (ministry)	**Application**	**Notes**
Ministry of Finance	taxation, payment	confidential tax number until 1985, and then public
Ministry of Social Affairs and Employment	registration of employment, social security contributions, benefits and facilities	also used since 1988 by the social security sector
Ministry of the Interior and Kingdom Relations and Ministry of Transport, Public Works and Water Management	identity (SOFI-number on passport and driving licence)	also used for the identity chain since 1996
Ministry of Education, Culture and Science	school funding and other applications	also used for the education sector since 2001
Ministry of the Interior and Kingdom Relations	identity (citizen service number on passport and driving licence)	the BSN has been the general personal number since 26 November 2007
Ministry of Health, Welfare and Sport	medical patient file	since 1 June 2008 the BSN has also been used as the unique personal healthcare number

This example illustrates how tempting it is in practice to adopt an already existing number in other sectors or chains as well. This appears to be an effective approach, but the (partly hidden) costs of shared use are often underestimated. This is because people often do not have a clear image of the increasing management problem and costs caused by multiple-chain usage. After all, a shared

number plays a different role in each chain. Moreover, each chain is affected by different chain-specific sources of contamination. In the case of shared use, this leads to unexpected management problems, because people in the one chain have no idea about the specific contamination sources and forms of fraud in other chains. That often results in errors beginning to accumulate, but then it often is too late to counteract the gradually deteriorating quality of the personal number system and the related files.

> *Example* **Look-alike fraud with a general personal number**
> If someone identifies himself to his employer in the Netherlands with the driving licence of someone else who resembles him (known as 'look-alike fraud'), his employer also registers the BSN of the official holder of that driving licence for the payment of income tax and social security contributions. No further checks are carried out, since that information is given in the driving licence.
>
> The fraudster remains invisible for the tax authorities even if the official holder of the BSN succesfully protests against these tax transfers and social contributions. A fraud in the identity chain thus has implications for the tax and social security chains that only come to light much later.
>
> Similarly, general usability increases the value of the number, which makes abusing that number more attractive. That is why a general personal number system is difficult to manage.

The adoption of already existing number systems usually throws up too many management problems. The starting point for a robust number strategy is therefore that number systems are chain-based and chain-specific, and that multiple-chain use is only advisable under special circumstances (see the next subsection 4.4).

4.4 Number system management

Number systems become contaminated by usage, by changed circumstances and sometimes by the mere passage of time. Writing errors are virtually inevitable. Some details change in the course of time. An incomplete statement sometimes results in a second number being issued to the same person. A different character set in an information system, only using capitals or without diacritic characters (č, g, œ, ů, etc.), for example, soon results in different wordings. The later registration of details containing writing errors or differences can result in the details of several people or social objects being erroneously registered under one number, or the details of a single person or object being registered under several numbers. Contamination of number systems is therefore not necessary deliberate. On the other hand, if the holder of a personal number has an interest in obtaining a second number or linking a detail to another number, there are in practice many ways in which this can be elicited. Improper usage or misuse can in turn result in new incorrect registrations and links. In practice, each chain has its own specific temptations and alternatives for improper use or misuse of a number. Numbers with a high economic or social value are extra vulnerable.

Table 3. The citizen service number (BSN) in five social chains.

Chain Requirement	Tax matters	Social security	Identity	Education	Healthcare
Purpose	registration, payment of tax	linking and (informal) recognition	linking and (formal) recognition	counting students	linking and (formal) recognition
Durability	duration of obligation to pay tax	period of a person's financial independence	permanent and long after death	school period	permanent
Error tolerance	fairly high	fairly low	very low	fairly high	extremely low
Risk of fraud	high	very high	high	low	fairly high

The necessary characteristics, the desired reliability and the administration requirements of a number system are dependent on the chain process and the requirements set for that number by the specific dominant chain problem. Table 3 gives an impression of the varied requirements for the BSN system by the different chains using it.

Based on this, we can identify various forms of management. In table 4 a distinction is made horizontally between passive and active management. The scope of the management activities is given vertically, from issuing a number to monitoring its use. That amounts to six different management regimes for number systems.

Table 4. Six management variants for number systems

	Passive	**Active**
Issuing	1 Allocation on request.	2 Allocation with legally-prescribed ID check based on documents and other data.
Administration	3 Registration of holder's details.	4 Registering holder's details, and periodically checking of the holder's rights, to prevent misuse.
Monitoring	5 Registering details about the use of the number and *registering* misuse or attempts at misuse.	6 Registering details about the use and registering misuse or attempts at misuse, and *combating* misuse, before and after.

Depending on the entire application and value of the number, a chain features some general but also some chain-specific sources of contamination and forms of fraud. A number administrator can prepare himself for this by making use of all chain-related self-cleaning and self-resolving mechanisms. Generally speaking, people opt for the simplest and cheapest management variant that meets the requirements. Management variant 1, for example, is therefore generally adequate for a temporary chain number for objects, whereas management variant 6 is perhaps more appropriate for the management of a permanent public personal number with substantial social value.

We are now able to define more clearly the adverse effects of multiple-chain use. Tables 3 and 4 showed that different chains set different requirements for a number and, accordingly, its management. Now that the citizen service number (BSN) is being used as a unique patient number in the healthcare sector, the very low error tolerance in medical chains calls for the most intensive management variant in table 4. The costs of this are in no way in keeping with the lighter management requirements in the tax and social security chains, where the adverse effects of extra fraud can be rationally weighed up against the additional costs of fraud prevention.

Similarly, general use increases the value of the BSN, which makes abusing that number more attractive with the most chance of success in chains with a weak management variant. Because the propagation of errors and risks from one chain to another is difficult to predict or manage, the requirements of the most vulnerable chain should be applied for the management of a general personal number system. There is usually a lack of support for the costs of this maximum management variant in sectors which themselves set less strict requirements. For this reason, in cases of multiple-chain usage one often settles for the minimum management variant, because this is being regarded as necessary by all using chains. This has serious implications for the more critical or vulnerable areas of the number system application.

Multiple-chain usage of a number system can only be an effective number strategy if:

- the requirements of various chains or sectors are comparable
- the value of the number is barely increased by the multiple-chain usage

- the chain-specific sources of contamination are similar
- the knock-on effects of errors and fraud from one chain to another are reasonable predictable and manageable.

Only under those circumstances, the number system can be managed optimally for several chains at the same time. An example might be the use of an education number for
(1) the funding of schools; the amount of money depending on the number of pupils (=education numbers),
(2) a national certificates registry, and
(3) the prevention of youngsters dropping out of the school system without a proper qualification.
Chain analysis should prove that multiple-chain use of a number system is adequate (Grijpink, 2010a).

Therefore, the key principle that number systems are chain-specific is related (among other things) to the ability to optimise management within the requirements of the chain. This key principle also implies that the multiple-chain usage of existing number systems will not usually be an effective number strategy.

4.5 Social effects of number systems (efficiency and privacy)

Two social effects of number systems are important within the scope of this article (Grijpink, 1999, p. 135): streamlining the exchange of information between autonomous organisations in chains and enhancing the protection of privacy when processing or exchanging personal data. In the years to come, (personal) numbers in electronic transactions will have an even clearer identification function than is presently the case. That is why compartmentalising the use of personal numbers with a view to protecting privacy is no less important than using numbers to prevent errors in chain communication. Therefore, both social advantages depend on the existence of chain numbers. As we shall see in subsection 4.6, that does however have implications for the use and management of general personal number systems.

4.5.1 Streamlining the exchange of information within a chain

Numbers are first and foremost important to streamlining the exchange of information between autonomous organisations in chains with the aim of structurally combating errors and chain failure. Numbers provide guarantees against writing errors and discrepancies, but there are many management routines available for numbers that are more difficult to put in place with text or images. A number system at chain level makes it possible to verify personal details for all chain partners collectively, without those details having to be placed in the parties' internal source registers.

With a number system and a reference index, for instance, it is also possible to put in place a wide range of chain alerts, as described elsewhere (Grijpink, 1999, 2010b). The result of this is that these chains function intelligently, without each of the parties having to create large databases that cannot be kept up-to-date and if used repeatedly can lead to erroneous decisions.

4.5.2 Enhancing the protection of privacy

Secondly, number systems offer ways of enhancing the protection of privacy when processing and exchanging personal data. When using a number system in a chain's information infrastructure, the protection of privacy can be structurally enhanced in two ways:

a. by having personal data registered and exchanged in the chain using the chain's own number as much as possible, the ability of the chain's own employees to link these personal data to details from other chains is structurally reduced. If more than the chain's own number is needed for a certain action, the number system can be used for the additional personal details. In the information society of the future, more attention will have to be paid to this *internal* protection of personal data. We are still concentrating too much on limiting the *external* exchange of data.
b. for communication between chains, the chain number of the demanding chain can be converted by a number administrator into the number of the chain on which the demand is being made, and vice versa. Numbers that are alien to the chain are thus prevented from spreading further, and the origin of a detail or a question can be screened off. If the criminal chain wants to find out whether a detainee is receiving benefits, the enquiries to the social security sector must be made with the BSN rather than the personal number of the criminal law chain. If this number was visible to bodies in the social security sector, everybody in that sector would be able to see that the person in question was about to be imprisoned for a longer period of time, while this information does not need to be further distributed (Grijpink, 1999, p. 138). And that is pre-

cisely what the privacy regulations guard against.

Properly managed chain numbers are therefore a future-proof starting point for all large-scale, national and international number strategies.

4.6 Type of number strategy: single, multiple or composite

In this subsection we develop a starting point for choosing between a single, a multiple and a composite number strategy. A *single* number strategy is one that works exclusively with a compulsory general public number. A *multiple* number strategy is based on a lot of unrelated chain numbers. The *composite* number strategy combines the two other number strategies.

However, as soon as the single and the multiple number strategies are combined, the synergy between the general and chain numbers begins to play a role. As is explained below, a composite number strategy for personal numbers is in fact conceivable, but not with a *compulsory* general personal number. So, choosing for a compulsory public general personal number blocks the way to any composite number strategy because the compulsory personal number drives out chain numbers.

Let us turn first to a more detailed look at the single and multiple number strategies.

If we have to choose between them, *a number strategy based on a lot of independent chain numbers* will be preferable. After all, chain numbers yield the most flexibility of use and facilitate the effective management of each number system within the constraints of its own chain. The advantages of chain-related self-cleaning and self-resolving mechanisms can be used to the full. The social or financial value for the holder is divided over several individual personal numbers, so that the value of each number remains low and each number is less vulnerable to misuse or attack. Chain numbers also facilitate streamlining chain communication and protecting our privacy. Chain numbers that are managed independently provide checking information for quality assurance and identity fraud prevention by the individual number administrators.

Opposed to this multiple number strategy is the *single number strategy with the compulsory use of a general public personal number* in a wide range of situations, regardless of the chain processes being supported, and regardless of the problems being solved by this number system. A personal number system of this type therefore lacks a direct relationship with a dominant chain problem, so that chain-related, self-cleaning and self-resolving mechanisms work less well. Making widespread use of the one general personal number increases its value, which makes it more vulnerable to attack, misuse and fraud. However, the available control information diminishes as chain numbers are displaced by the general personal number. Thus, fewer independent chain number systems remain in place for quality protection and identity fraud prevention. At the same time, number management automatically seeks the lowest point: although the number management must – as we have seen – be directed at the most demanding chain that it serves, it is often the case that there is no support for the extra costs involved, so that in practice we make do with a minimum management effort.

The *composite number strategy* combines the advantages of both the single and the multiple number strategies. With the composite number strategy we make use of both independently managed chain numbers and more general personal numbers, in an evenly balanced mix. Number administrators can compare chain numbers with each other, with one or more general personal numbers helping to establish whether the right person has been identified. That makes it possible to expose identity fraud and protect vulnerable data sets against contamination. For general personal numbers to be used for this purpose we have to choose numbers that will not harm or displace chain-related personal numbers, but which could actually increase the reliability of chain-related personal numbers. A *compulsory* general personal number is not suitable for that purpose because a number system of that nature inevitably displaces chain numbers, leaving us with a single number strategy! The composite number strategy is thus only stable over a longer period of time if using the general personal number is not compulsory.

Example **The Dutch model versus the Austrian model**

The Dutch BSN number strategy (May 2012) can be described as a single number strategy based on a compulsory general personal number, the BSN number. There are some exceptions giving rise to a (very) light version of a composite number strategy. Indeed, the BSN can be overruled in a specific chain, but only if there is a statutory provision for the chain number with precedence over the BSN. Only then the BSN Act provides for some space for quality monitoring and identity fraud prevention with both personal numbers and related personal data.

The Austrian model opts for a multiple number strategy based on a number of chain numbers derived from the sourcePIN (ssPINs) which cannot be traced back to each other. For government use only, the law provides for verification against the SourcePIN and between the derived ssPINs in a secure environment within the government. Seen from the government perspective as well as from the citizen, the Austrian national personal number strategy can be considered a composite number strategy.

The key principle here is that a complex information society calls for a composite strategy for personal numbers. The emphasis should be placed on chain numbers. If necessary, chain number administrators can resort to cross-checking by authorised bodies. This results in a robust conglomerate of personal numbers that is up to the increasing demands of reliability and safety in an information society without borders.

4.7 Development patterns of number systems

From Table 2 and 3 (see subsections 4.3 and 4.4) a model of the development of a number system can be derived which is presented in Table 5. This model follows the logical sequence of development stages of a number system from phase 1, in which it is used as an internal number by an organisation, to phase 7, with formal, public general usage, with collective, independent management. The dynamic that ensures that a number system grows from the one development phase to the other arises mainly from the improper use and misuse of numbers and from the export of a number system to other sectors. That is why the *logical* sequence of the development steps shown in table 5 is not often seen in practice. The interplay of forces in practice results in a more zigzagging *chronological* growth pattern.

Table 5. Growth path of a number system

Phase	Scope of application	Functions
1	internal use	registration
2	public number with chain usage, but without collective, independent management	an initially sheer administrative number often develops into an informal tool for identifying something or somebody
3	public chain number with collective, independent management	in this phase the administrative number develops into a formal aid for identifying something or somebody
4	informal multiple-chain usage	used informally by other chains, e.g. for verification (functions in the other chains as an 'internal' number, see phase 1)
5	formal multiple-chain usage	officially adopted by another sector as its own number (see phase 3, the process repeats itself)
6	informal, non-public general usage, without collective and independent management	the general number is not public and is used by the authorised bodies as an internal number of comparing details from several chains
7	formal, public general usage, with collective and independent management	the number serves as a public, general identification point

Phase 1: The internal use of number systems phase. An example of a phase 1 number system is the tax number when it was only used as an internal registration number for tax authorities and could not be called up.

Phase 2: This phase begins with the disclosure of a number, after which it is used chain-wide without there being a collectively managed chain-specific information infrastructure. That is a characteristic of phase 3. The number system first functions as an administrative number, but it can gradually develop informally into an aid to identifying people or objects.

Phase 3: The third phase is typified by a formal, public chain number. An example of this is the internet IP address system, which is used to transport packets of information from one connection to another. That number system is collectively managed, independently of the individual interests of an internet service provider (ISP). The telephone number is another public number in phase 3, with collective management in development, which has formally gained an identification function since the introduction of the call ID system. The Austrian ssPIN system fits within this phase.

Phase 4: This phase is characterised by informal multiple-chain use. The postcode-house number system is a number system at chain level in this phase because it is informally used by other sectors for verification purposes. In this context, 'informal' means that individual partners from other chains use a number without this use in that other chain developing into a generally accepted method.

Phase 5: Formal multiple-chain usage. This was the case for the SOFI-number in the period from 1998-2007.

Phase 6: Informal general usage. The Netherlands already has some non-public, general number systems that are used as internal numbers for comparing details form several chains, such as the A-number of the Dutch municipal residents' registry (GBA). The Austrian sourcePIN forms another example.

Phase 7: In this phase the number formally serves as a public, general identification point. The Dutch citizen service number (BSN) has been in this phase since 2007.

5 A step-by-step plan for a number system

By way of a summary of the various aspects covered in sections 2-4, this section presents a ten-steps-procedure for the design, implementation and management of a (personal) number system that can also serve as a framework for assessing existing number systems.

5.1 What do the parties involved want to use the number system for? Which characteristics does the number system need (section 2: function, area of application, unicity, scope and significance of numbers)? Benefit from the wide range of alternatives so that the number can meet the requirements for a long period of time. Also consider easily transferable visible information in a number and the use of verification methods within the number to avoid writing errors and to check for feasibility. Do not opt for a permanent number if a temporary one is sufficient. If the number system must remain in place for a long period of time, take account of the increasing size of the target group, especially if it is meant to become a non-interoperable personal number system within the EU (subsection 4.1).

5.2 Does this concern a personal number that will form a personal detail as seen from the application as a whole (section 3)? If not, there are no special legal restrictions. If so, can the number be used anonymously or pseudonymously? If so, that is the preferable option. If not, the requirements of the privacy protection law apply (section 3: look separately at the objective, proportionality and subsidiarity, target group, voluntary nature, scale of application, central versus decentral storage of the number, shielding and encryption of personal numbers and independent supervision). Privacy laws set additional requirements for sensitive personal data (the number contains, for instance, information about somebody's race or origin).

5.3 *Vertical* positioning (subsection 4.1) is possible at a minimum of three different levels. Look first at chain level. If it can maintain itself there in a stable manner (see 5.4) that positioning is preferable. The *horizontal* positioning (subsection 4.1) calls for a solution for similar numbers from other domains or countries. An interoperable setup is preferable for large-

scale national (personal) number applications. If it does not prove possible to incorporate similar numbers from different domains or countries using a different method (compare the Austrian model), make sure that there are sufficient numbers, *also in the long term!*

5.4 Chain linkage is an important starting point for all number strategies (subsection 4.2). In which social chain must the number system play a role? Which role? Is the number system necessary to the chain-wide approach of the dominant chain problem? If not, consider an internal number system and have one of the parties manage that number system. If so, it is a public chain number. In that case, make arrangements for professional, independent chain number management.

5.5 What type of management is required? In practice there are at least six different forms of management (subsection 4.4). Choose the simplest and least expensive form of management that meets the requirements. In this context, pay attention to the requirements that arise from the role that the number will play in the chain, the value of the number in the eyes of the holder and chain-specific sources of contamination and fraud types.

5.6 Can other number systems be used for verification and management? Develop an effective system to compare numbers. NB: this is not multiple-chain usage as meant in subsections 4.3 and 4.4, because one does not discard the chain's own number system.

5.7 Chain linkage is a good starting point for *all* number strategies. Multiple-chain usage results in many additional management problems. Shared use of an already existing number can be a good number strategy (subsections 4.3 and 4.4), but only if:

- the requirements of various chains are comparable;
- the value of the number is barely increased by multiple-chain usage;
- the chain-specific sources of contamination are similar;
- the knock-on effects of errors and fraud from one chain to another are reasonably predictable and manageable.

If in doubt, do chain analyses for every chain (Grijpink, 2010a).

5.8 Number systems have two important social effects: they streamline chain communication and protect privacy (subsection 4.5). Does the application of the number system promote fast and accurate communication in the chain to tackle the dominant chain problem together? If not, develop some chain-computerisation solutions on the basis of the chain number (Grijpink, 1999, pp. 19). Does the application of the number system in the chain promote the protection of privacy through registration and communication by number without additional personal data so that personal data are internally protected? When enquiries are to be made in another chain, will the specific chain number be replaced by the chain number of the chain at which the enquiry is made (and vice versa)? This way, people are unable to obtain information that they do not need to know.

5.9 A single number strategy appears to offer an inadequate basis for large-scale public personal numbers in a complex information society (subsection 4.6). Pay special attention to the protection of the original personal number (compare the Austrian model). Consider a composite number strategy, but make sure that using the general personal number is not made compulsory.

5.10 It turns out that there is certain logic in the development pattern of a number system (subsection 4.7). This can help in selecting a number system or a number strategy. A step back in the logical line of development is perfectly feasible, but skipping a development phase will not usually meet with success.

Biographical note

Jan Grijpink (1946) is Emeritus Professor, Utrecht University and senior advisor of The Expertise Center, IT consultants for government, in The Hague. Since October 2006 he has been chairing the Netherlands Biometric Forum (NBF). He is editor-in-chief of the e-Journal of Chain-computerisation. http://jcc.library.uu.nl

From 1995-2011 he was Principal Advisor at the Dutch Ministry of Justice, with a special focus on information strategy and identity issues.

He studied Economics (1969) and Law (1971) at Groningen University and earned a postgraduate degree in Organisation & Management Science (S.I.O.O. Utrecht) in 1976. In 1997 he obtained his doctorate at Eindhoven Technical University with a thesis about Chain-computerisation.

Jan Grijpink regularly publishes on chain and identity issues in a complex information society focusing on large-scale information systems and chain interdependencies.

Literature references

Blocksma, M. & Van Maanen, H. (1990). *De Schaal van Richter en andere getallen*. [*Reading the numbers*.] Amsterdam: Bert Bakker.

Grijpink, J.H.A.M. (1997). *Keteninformatisering. Met toepassing op de justitiële bedrijfsketen. Een informatie-infrastructurele aanpak voor de communicatie tussen zelfstandige organisaties.* [*Chain-computerisation. Applied to the Criminal Law Enforcement Chain. An information-infrastructural approach to the communication between autonomous organisations*.] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (1999). *Werken met Keteninformatisering. Informatiestrategie voor de informatiesamenleving*. [*Chain-computerisation in practice. An information strategy for an information society*.] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (2000a). Chain-computerisation for interorganisational policy implementation. *Information Infrastructures & Policy, 6*, 81-93. Amsterdam: IOS Press.

Grijpink, J.H.A.M. (2000b). Chain-computerisation for better privacy protection. *Information Infrastructures & Policy, 6*, 95-107. Amsterdam: IOS Press.

Grijpink, J.H.A.M. (2002a). *Informatiestrategie voor Ketensamenwerking: Keteninformatisering als visie, resultaat en methode*. [*Information Strategy for chain co-operation. Chain-computerisation as perspective, result and methodology*.] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (2002b). Personal numbers and identity fraud: Number strategies for security and privacy in an information society (Part I and II). *Computer Law and Security Report*, 18 (5 and 6), 327-332 and 387-395. Oxford, UK: Elsevier Science Ltd.

Grijpink, J.H.A.M. & Prins, C. (2003). New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity. In C. Nicoll, J.E.J. Prins & M.J.M. van Dellen (Eds.), *Digital Anonymity and the Law: Tensions and dimensions*, pp. 249-269. The Hague: TMC Asser Press.

Grijpink, J.H.A.M. (2004). Identity fraud as a challenge to the constitutional state. *Computer Law and Security Report, 20*(1), 29-36. Oxford, UK: Elsevier Science Ltd.

Grijpink, J.H.A.M. (2008). Biometrics security. Trend report on biometrics: Some new insights, experiences and developments. *Computer Law and Security Report, 24*(3), 261-264. Oxford, UK: Elsevier Science Ltd.

Grijpink, J.H.A.M. (2010a). Chain Analysis for Large-scale Communication Systems: A Methodology for Information Exchange in Chains. *Journal of Chain-computerisation, 1*.

Grijpink, J.H.A.M. (2010b). *Keteninformatisering in kort bestek. Theorie en praktijk van grootschalige informatie-uitwisseling*. 2nd edition. [*Chain-computerisation in brief. Theory and Practice of large-scale information exchange*.] The Hague: Boom/Lemma Uitgevers.

Hayat, A., Posch, R. & Rössler, T. (2005). Giving an interoperable solution for incorporating foreign e-ID's in Austrian E-government. *Proceedings of IDABC-Conference 2005: Cross-Border e-Government Services for Administrations, Businesses and Citizens*, pp. 147-156. Brussels: European Commission. http://ec.europa.eu/idabc/en/document/3910/5803#proceedings.