Giving an Interoperable Solution for Incorporating Foreign e-IDs in Austrian E-Government

IDABC Conference 2005
18 February 2005

Thomas Rössler
About A-SIT

Secure Information Technology Center – Austria

- **Founded:** 1999
- **Business Fields:**
  - Attestation of Certificate Service Providers according to the EU Directive on Secure Electronic Signatures (1999/93/EC)
  - Austrian E-Government Initiative
  - Consulting in questions of IT-Security
  - Attestation of Online Payment Systems

Secure Information Technology Center – Austria
Content

- Austrian Identification System
- Austrian Citizen Card Concept
- The Integration of Foreign e-IDs
- Conclusions
Content

- Austrian Identification System
- Austrian Citizen Card Concept
- The Integration of Foreign e-IDs
- Conclusions
The Austrian Identification System – in General

- Identification is based on unique identification numbers taken from Austria’s base registers:
  - e.g. Central Residents Register (CRR), etc.
- Every person in Austria is registered with such a base register
- Even foreigners living in Austria can be registered with the so called Supplementary Register (SR)

Every person gets assigned a unique personal identification number, the so called Source PIN
The Austrian Identification System – the **Source PIN**

The Creation of **Source PINs** based on the identifiers of Austria’s base registers:

1. **CRR** and **SR**
2. Convert into binary representation
3. Add a secret seed value
4. Encryption by applying a secret key (3DES)
5. BASE-64 Encoding
6. **Source PIN (sPIN)**

Identifiers are publicly available

**Source PIN** is kept secret
The Austrian Identification System – the **Source PIN**

- **Source PIN**
  - … is *unique*
  - … in contrast to other base identifiers, it is under the *sole control* of the citizen
  - … it *must not* be stored by any governmental or private party
- Due to privacy reasons, the **Source PIN** is not used to identify persons in E-Government processes

*For Identification in E-Government Processes, we use*

**Sector Specific-PINs (ssPIN)**
The Austrian e-Identification System – the **Sector Specific PIN**

- Each governmental sector (i.e. different areas of the public administration) is assigned a specific alphanumeric code, the sector code.

- For each of these sectors, the Austrian e-ID concept foresees a separate unique identifier, which is called the **Sector Specific PIN (ssPIN)**.

- The **Sector Specific PIN** is derived from the person’s **Source PIN** by applying a cryptographic one-way function (Hash-function).

> Each ssPIN is different and it is neither possible to calculate the underlying sourcePIN nor any other sector’s ssPIN from a given ssPIN.
The Austrian e-Identification System – the **Sector Specific PIN**

For Example:

1. **Sector „Taxes and Duties“**
   - **SA**
   - Add Sector Identifier (SA) to the sourcePIN (Concatination)
   - One Way Function HASH-Function (SHA-1)
   - ssPIN for Sector SA

2. **Sector „Social Security“**
   - **GH**
   - Add Sector Identifier (GH) to the sourcePIN (Concatination)
   - One Way Function HASH-Function (SHA-1)
   - ssPIN for Sector GH
Content

- Austrian Identification System
- Austrian Citizen Card Concept
- The Integration of Foreign e-IDs
- Conclusions
Austrian Citizen Card Concept

- **For Identification:** Source PIN → Sector Specific PIN
- **For Authentication:** Electronic Signatures

---

Citizen Card

- Citizen is **identified** uniquely (ssPIN)
- and **authenticated** by applying electronic signatures
Content

- Austrian Identification System
- Austrian Citizen Card Concept
- The Integration of Foreign e-IDs
- Conclusions
The Integration of Foreign e-IDs

- Austrian E-Government Act says that a *recurring identity* can be created for foreigners without having registered with an Austrian base register.

- Requirements for a recurring identity:
  - *… electronic signatures* according to 1999/93/EC
  - *… a unique identifier* preferably taken from the foreigner’s local e-ID
  - *… as a unique identifier, the certificate’s serial number* can be used as well

- What has to be done:
  - create a *Substitutional Source PIN*
  - combine *Substitutional Source PIN* with the public key used for electronic signatures and create an Identity Link
The Integration of Foreign e-IDs

- We have developed a prototypical web-service which allows to request for creating a *Substitutional Source PIN*

- So we could create recurring identities based on the e-IDs of
  - Italy (Carta d'Identita' Elettronica)
  - Finland
The Integration of Foreign e-IDs

**Finish e-ID**
- Gain Certificate Data (e.g. Serial Number) – Concatinate it with "FI:"
- Applying a keyed Hash-Function (HMAC)
- BASE-64 Encoding
- Substitute Source PIN (subsourcePIN)

**Italian e-ID**
- Gain Tax-Number – Concatinate it with "IT:"
- Applying a keyed Hash-Function (HMAC)
- BASE-64 Encoding
- Substitute Source PIN (subsourcePIN)
The Integration of Foreign e-IDs

As a result: foreign e-IDs can be used in Austrian E-Government applications as a recurring identities.
Content

- Austrian Identification System
- Austrian Citizen Card Concept
- The Integration of Foreign e-IDs
- Conclusions
Conclusions

- The Austrian e-ID system bases on personal unique identifiers – **Source PINs**
- For authentication **electronic signatures** are used
- To integrate foreign electronic identities a **Substitutional Source PIN** has to be created
- By the use of a **Substitutional Source PIN** and **electronic signatures** foreigners can participate in Austria’s E-Government
Thank you for your attention…

Thomas Rössler
thomas.roessler@a-sit.at

Secure Information Technology Center – Austria