



Handy, NFC, RFID and chaotic storage

Carlo U. Nicola,
Institut für mobile und verteilte Systeme (IMVS),
Fachhochschule Nordwestschweiz (FHNW)

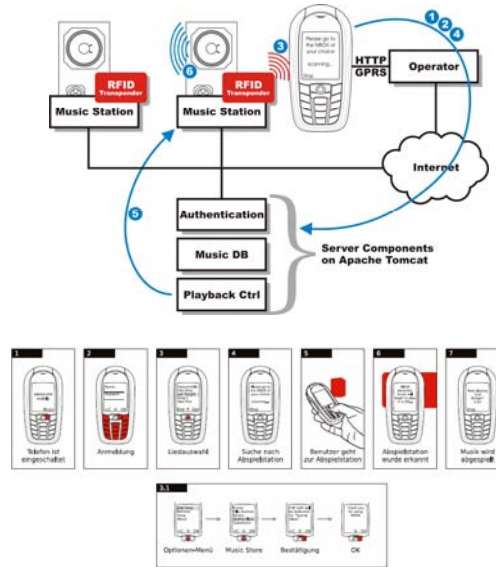
Topics

Q: Can Alice communicate securely with Bob via NFC/RFID technology in a practical application?

Steps toward a response to this question:

1. Music on demand with NFC/Handy authentication
2. Authentication with challenge/response
3. Problems with challenge/response protocols
4. The smart tools' cabinet
5. Problems and (tentative) solutions for a future chaotic storage management tool.

The first steps: Music on demand



FSC 6.3.2009 3

Authentication via challenge/response protocol

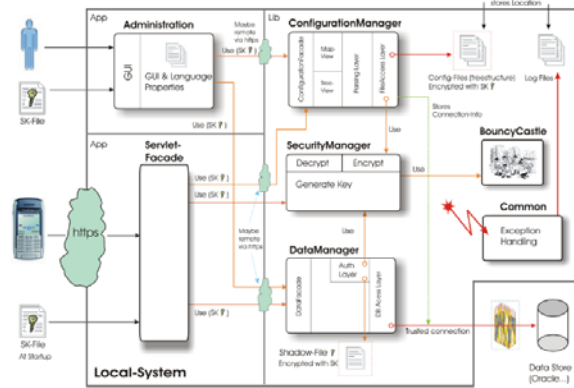


The different phases of the challenge/response protocol:

2. Server A gets password of B via shadow file;
3. Server A generates a random number RAND (the challenge) sends it to B;
5. B receives it applies one-way-function with key to it, gets a number RES (the response) and sends it back to A.
7. A checks if RES can be generated from RAND via one-way-function and shared key.

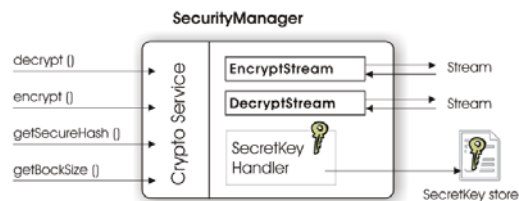
FSC 6.3.2009 4

The back office: Server A



FSC 6.3.2009 5

Session key for A ↔ B data exchange



A good protocol should:

1. Negotiate **cryptographic** parameters
2. Establish a **shared** secret with the participation of both participants in the communication
3. Authenticate **endpoints**

FSC 6.3.2009 6

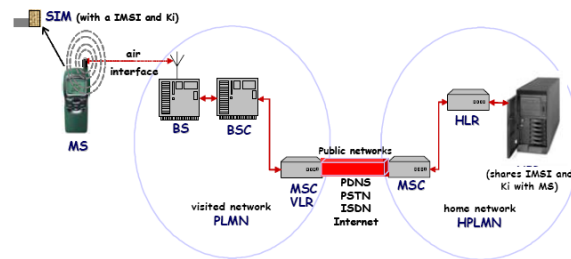
Problems with challenge/response protocols

1. It needs a long term shared key between server A and users B_i
2. It is extremely difficult to produce really good random numbers for the challenge
3. The logistics of distributing shared secrets is not only costly but also the costs grow with n^2 (where n is the number of users) .

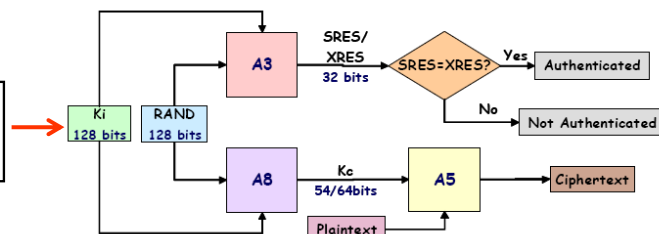
GSM is one well known practical application that somehow masters these difficulties.

FSC 6.3.2009 7

GSM/SIM recap



Part of the long term key is used to build the session key!



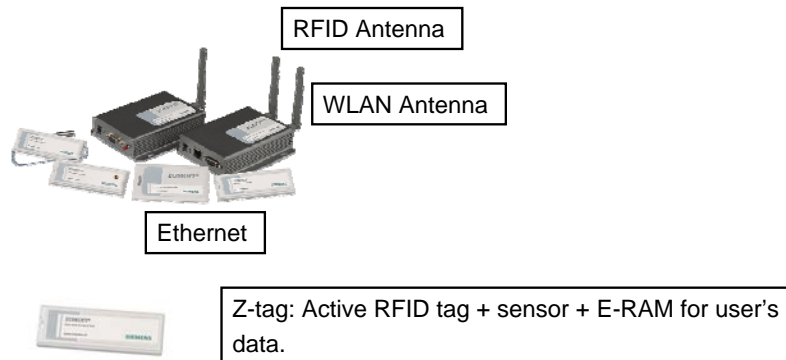
FSC 6.3.2009 8

The smart tools' cabinet

The problem: A firm XZ AG uses a typical LISTA cabinet to store semi-finished medical prostheses whose surfaces are polished and customized on order. These pieces are very valuable and all their movements should not only be automatically actualized in a DB but also only authenticated and authorized personnel should be involved in their movement.

FSC 6.3.2009 9

Solution's step one: Track



Track: Each prosthesis is bound to a Z-tag within a Lista cabinet. Each cabinet is also tagged with a Z-tag and a Z-controller guards one or more cabinets.

FSC 6.3.2009 10

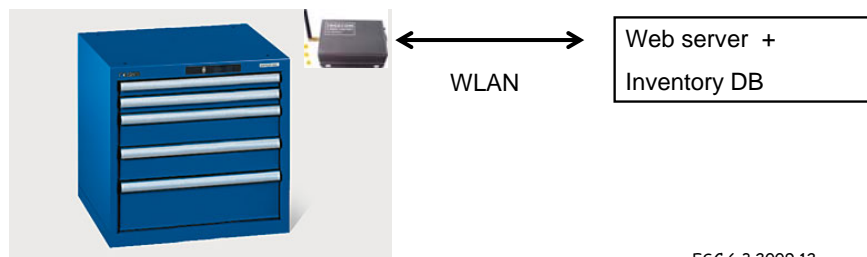
Solution step one: Track's hardware

1. **Unique ID for each Z-tag:** The ID is used to reference an object, asset or person. The length is 8 bytes and so it spans a large enough number space ($1.844 * 10^{19}$).
2. **User data:** 112 byte are free for storing user's specific information. The read and write cycles take a few ms per 8 byte. The length of transmitted packets is variable.
3. **Detection's range:** The Z-Tags transmit their data indoor as far as 80m (outdoor as far as 160m). This range is dependent on material, room geometry and antenna selection.
4. **Presence:** Each Z-Tag transmits its ID regularly so that the presence/absence of a tagged object is indicated. Additionally user data and sensor values (optional) can be transmitted on demand.
5. **Adjustable beacon rate:** The frequency of the data transmissions can be adjusted for each Z-Tag individually. This works over the air and at any time the Z-Tag is in reach. The beacon rate is programmable in steps, from 1,2,4,8,15,30 or 60 seconds.
6. **Size of zone:** The radius of a monitored zone can be adjusted in 32 steps.
7. **Mute tag:** Each Z-Tag can be "muted" individually. Like this, any transmission from the Z-Tag is stopped. By command from any Z-Controller the Z-Tag can be reactivated "over the air".
8. **Long battery life:** The battery life of the Z-Tags is **4 to 8 years**, depending on beacon rate and usage.
9. Z-tags work well even within metal cabinets.

FSC 6.3.2009 11

Solution step two: Trace

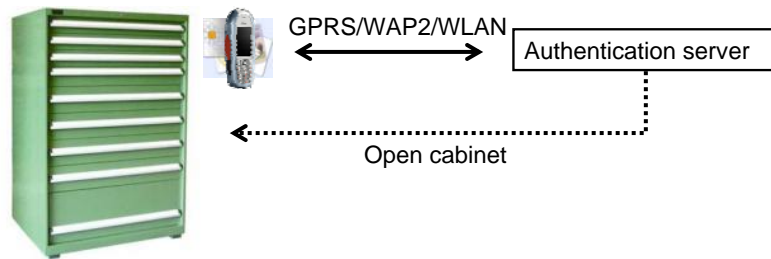
Trace: As soon as a cabinet's drawer is opened the actual state of the drawer's contents are transmitted via WLAN to a Web server + DB. This information is compared with the content of the last material movement in the same drawer and thus validated and updated. When the drawer is closed (by the authenticated and authorised personnel) the same process happens and if the technician has taken out some material the DB is updated. The whole history of these materials' movements are of course available in the DB.



FSC 6.3.2009 12

Solution step three: Authenticate + open cabinet

Authenticate: The technician that wishes to take out some material from the cabinet must be authenticated. He activates the application on his/her handy (password, special token, fingerprint, etc.) and via NFC interface on one side of the cabinet, his handy picks up the cabinet ID and sends the challenge to the authentication server via GPRS. In the same manner as in the music juke-box discussed before, if the authentication is successful, then the authentication server sends the signal to open the cabinet.



FSC 6.3.2009 13

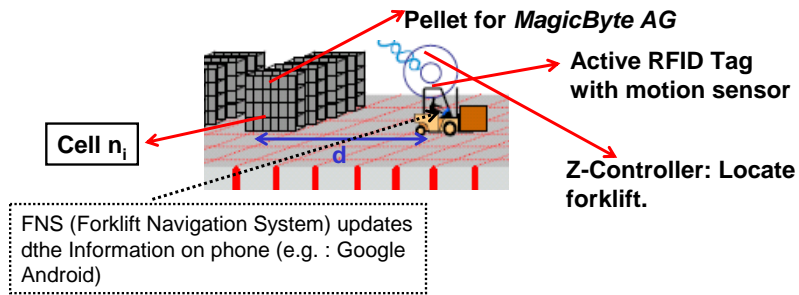
The storing principle of the future: Chaos

Storing principle: With RFID identification and localization it is not necessary to know exactly where we physically put material in storage. The system can always track down the zone within which the cabinets with the relevant material lies.

Chaotic organisation creates efficient order

FSC 6.3.2009 14

Forklift Navigation System in a chaotic storehouse



Big question: How secure can this solution be?

FSC 6.3.2009 15

The (insoluble) covert channel's problem



HAL: The man in the middle as lips' reader

2001 Space Odyssey: Stanley Kubrik

FSC 6.3.2009 16