Deusto
University of Deusto

Deusto Tech
Computing

ANNUAL SRII GLOBAL CONFERENCE
July 24-27, 2012

Service Authentication via electronic identification cards

Igor Ruiz-Agundez and Pablo G. Bringas

Guess how?

Identity is personal and cannot be transferred

Identifying the users of a service in the Internet is not an easy task

Existing authentication methods

Fingerprints

Passwords

Challenge response

Tokens

And so forth

Governments all over the world are working in secure access to e-government services

In this research we used the DNIe The Spanish authentication eID card

The DNIe offers

Authentication

Digital signature

Time stamping

Data integrity

And so forth

Facts about the DNIe

More that 29 millions of DNIe have been issued

The services and applications that make use of it is growing every day

15 European countries use eID cards
Many others are considering their development

Paradigms of authentication

Knowledge factors

Ownership factors

Inherent factors

Known factors

The DNIe is standard

It accomplishes the specifications

- ISO 7816
- PKCS#15

They specify how to operate with the keys, certificates and data

Security levels

Public zone

Private zone

Secure zone

Public zone level

It does not have security control

It stores the certificates of the root CA and the validation authority

Private zone level

It requires a password

It stores the user certificates for authentication and signature

The certificates never leave the inside of the DNIe

Secure zone level

It requires administrative privileges

It requires special physical

It stores personal information, fingerprint, photo and handwritten signature

Additional physical security

INVISIBLE

PATTERNS

SILKSCREEEN INK IRIS

KINEGRAMS PHOTOGRAPHY

PRINTING EMBOSSED

OFFSET TEXT IMAGES

GUILLOCHE MICRO-TEXT

POSITIVE CHANGING

ENCODED NEGATIVE

COLOUR

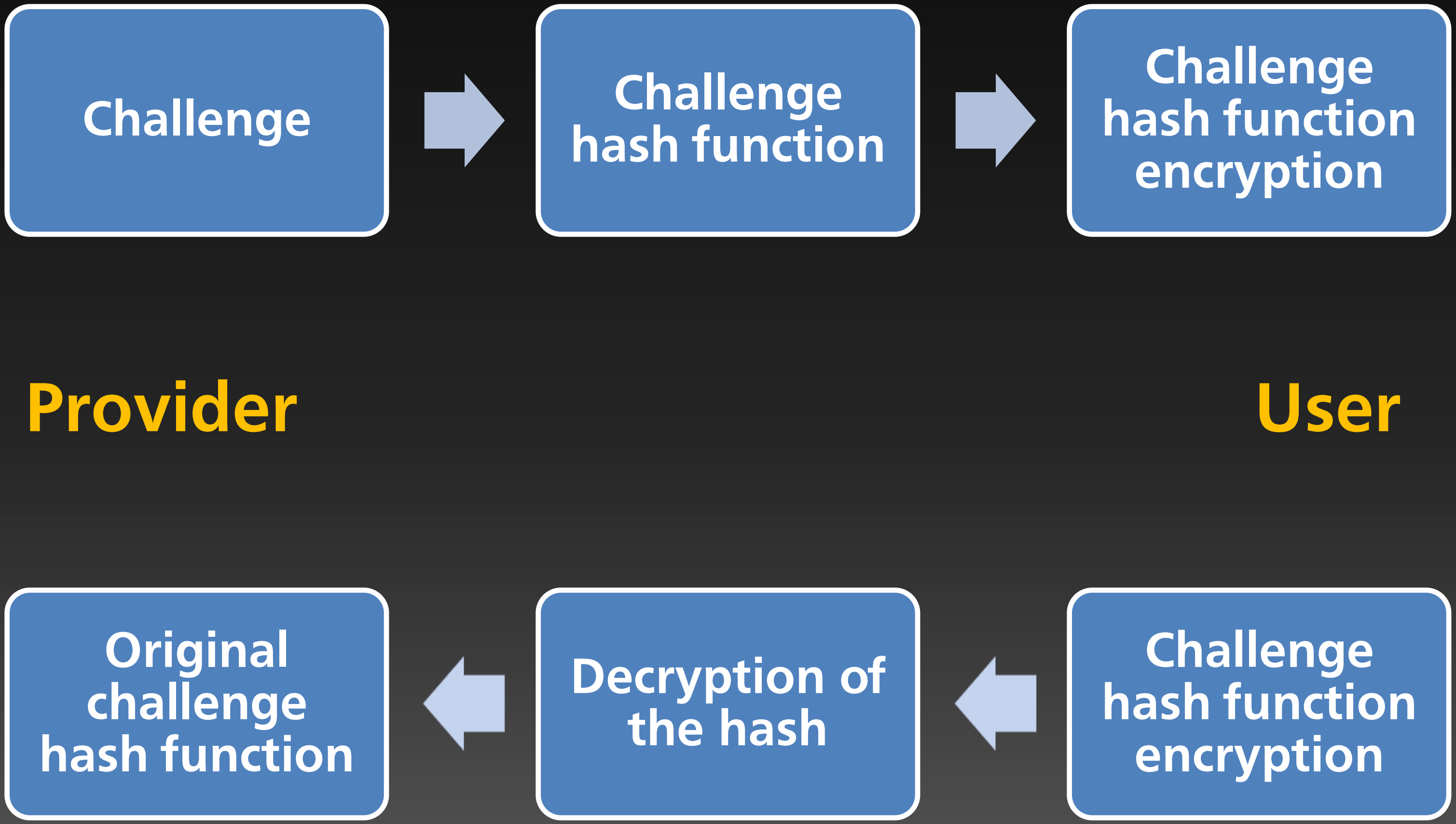
Scope

The DNIe can be used for information signing, time stamping, integrity guarantying and authentication

Authentication

The user has to prove her identity against a provider prior to make use of a service

Challenge-response authentication



Provider

User

Challenge

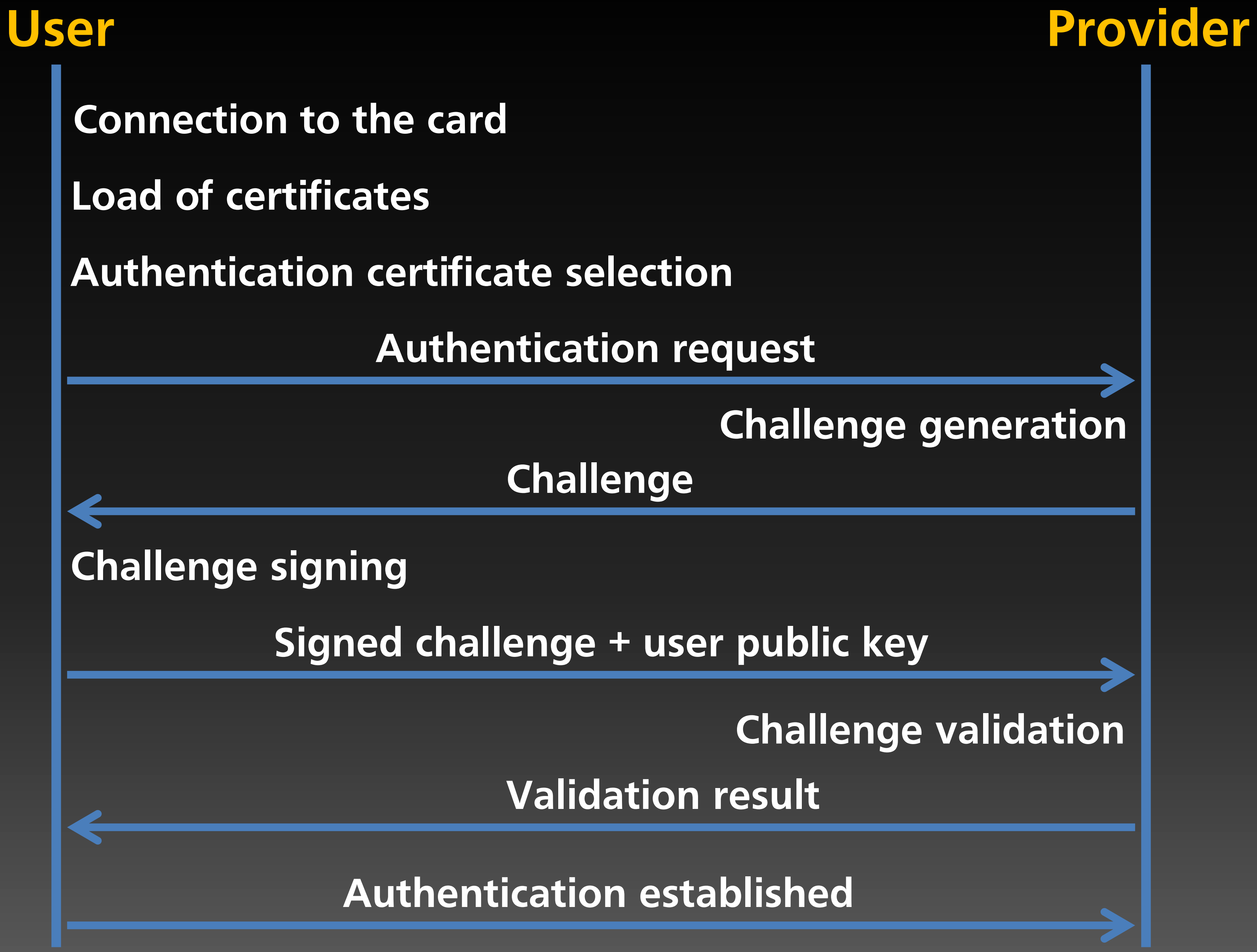
Challenge hash function

Challenge hash function encryption

Challenge hash function encryption

Decryption of the hash

Original challenge hash function



User

Provider

Connection to the card

Load of certificates

Authentication certificate selection

Authentication request

Challenge generation

Challenge

Challenge signing

Signed challenge + user public key

Challenge validation

Validation result

Authentication established

Evaluation

We integrate a DNIe authentication library in a VoIP service

VoIP Service

It enables sending and receiving call, transferences, call waiting, call-centre, and so forth

VoIP Service + Authentication

It provides authentication through the DNIe to the service

Currently in production in various call-centres

VoIP Service + Authentication

It enables unequivocal identification of the call-centre operators

It authenticates all the performed operations

Conclusions and future work

1

Introduced the related work in service authentication using eID cards

2

A multiplatform and multiservice authentication method through the DNIe or any eID card

3

Evaluation of the method in a VoIP service

Future work includes the support of other eID cards and services

Deusto
University of Deusto

DeustoTech
Computing

ANNUAL SRII GLOBAL CONFERENCE
July 24-27, 2012

Service Authentication via electronic identification cards

igor.ira@deusto.es