DIVERSID AUTHENTICATION SYSTEM PRESENTATION

Awarded silver medal at the International Exhibition of Inventions, Techniques and New Products GENEVA-2003

System registered under Patent 02748876.6

Introduction

There are still several issues about the necessary authentication in many of the dialogues taking place at a distance (internet, payment at e-commerce, ATM transactions, help desk assistance, ...).

At present, there are good solutions using different keys for each operation carried out, but:

- in most of them, only the originator of the dialogue is identified, assuming as correct the identity of the called party (not eliminating the problem of a possible personality fraud)

- it is very frequent to use keys with limited validity time (often insufficient if communication lines are slow or saturated)

What is new about the solution?

- Participants in an operation use keys only known to them, which they find available from a key storage device

- It uses keys which validity time is unlimited (values are not obtained from a temporary variable) but they are used only once and will be not used again

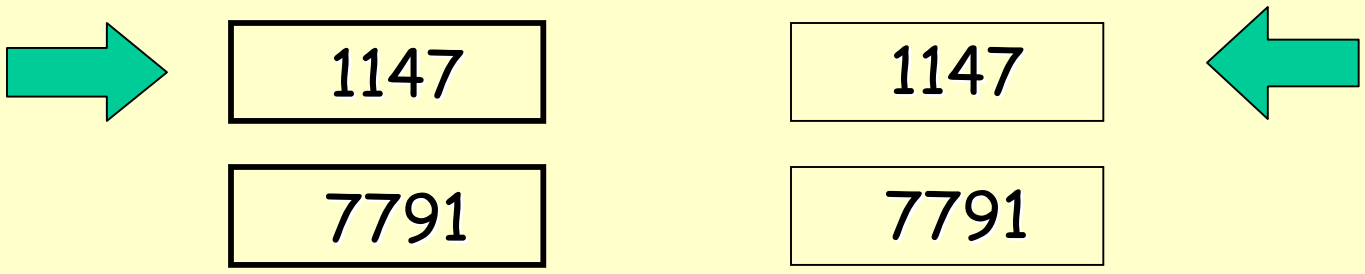
- Each non-presential operation uses at least three keys to carry out the authentication of the participants. For the next operation to be performed, keys will be new for the authentication process

- It does not consider the called party as identified until one of the keys reserved for such purpose is received from that side at the end of the operation in progress. This way, authentication process is completed while user trust in the system is generated, as he/she realizes that the other participant is sending the key he/she expects

- As several keys are used for each operation, part of them can be used for encryption of information

What is the procedure?

- An interchange procedure of keys that have been previously obtained in a random manner and stored in a device, grouped in packages.
- Each device, with its key packages, makes available to two or more people such stored keys so that they are shared and interchanged during the dialogues taking place between the parties, using one key package for each dialogue.
- When a package has been used already, it is marked in order to avoid its reutilization.
- Normally, one of the parties taking part in the dialogue will own the device, and the other one will have, using the most convenient means, a copy of the key packages stored in the device, as follows:

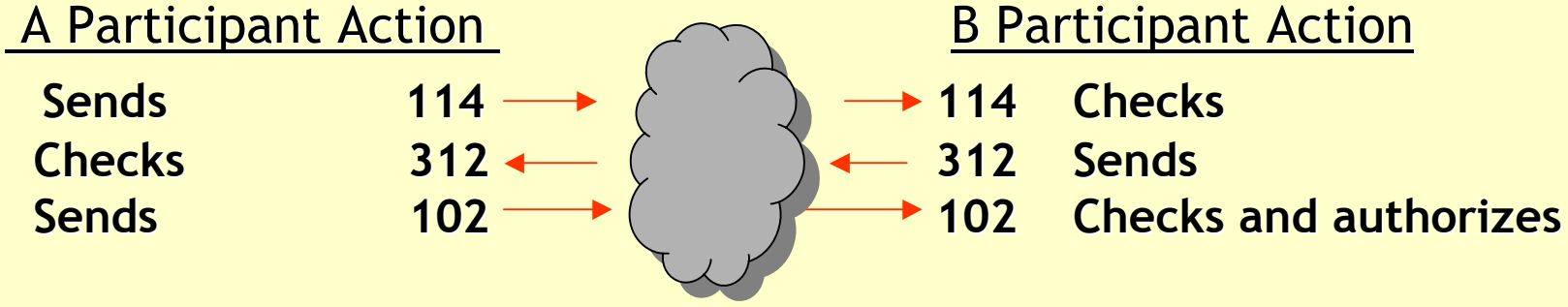


What is it used for?

For the identification of each of the participants in dialogues where there is physical distance between them, ensuring that the parties really ARE who they claim to BE. Simultaneously, it ensures the users' identity and sensitive information are protected throughout all dialogues.

Example of dialogue between two participants, A and B:

Key package shared by A and B {114,312,102}



Main characteristics of the system

- The size of the device in which keys are stored can be similar to the size of a credit card, which makes it easily portable.

- Other existing devices like, for instance, a mobile phone, can also be used as key storage and management devices.

- In order to access the stored keys, it is necessary to know the access code for the device.

- Key packages are made up of several randomly obtained digits.

- Each key package is used in only one dialogue, remaining as not available once it has been used.

- Digits forming the keys are not obtained from either any temporary variable or algorithm, which avoids finding out new keys from a set of known ones.

DIVERSID AUTENTICACIÓN

Main characteristics of the system

- As it does not use any temporary variable, there is no limitation with regards to key validity time and therefore neither there is for the response time to the messages making up the dialogue.

- The system allows scalability and adapts to the security level of the environment in which the dialogue is taking place, by fixing both the keys' length and the appropriate number of digits to interchange.

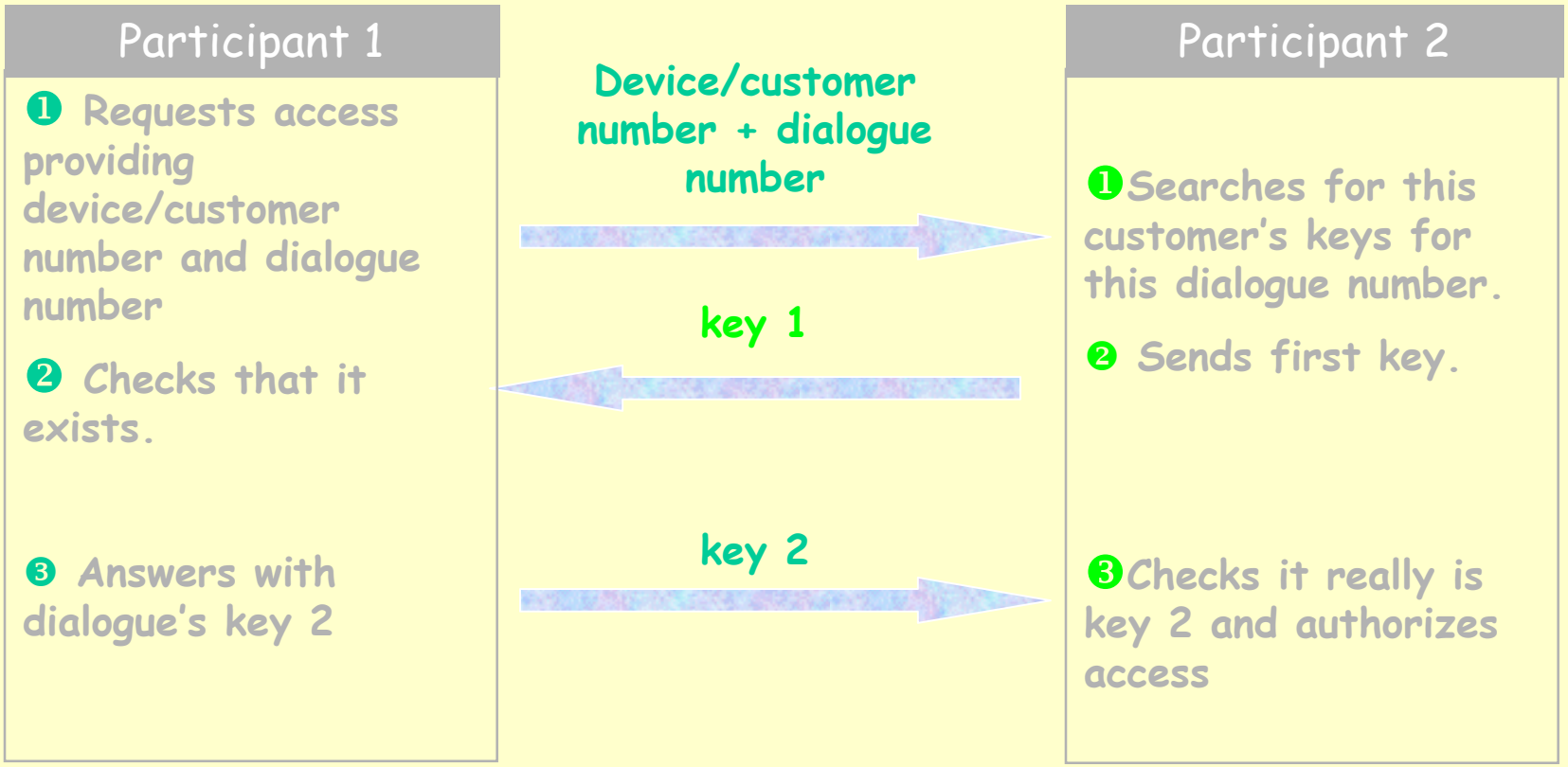
- Authentication is complete because all participants in the dialogue are truly identified.

- The system allows authentication for dialogues in which more than two participants intervene. It offers a distinct peculiarity though, as none of the participants knows all keys needed to complete the dialogue.

How does it work?

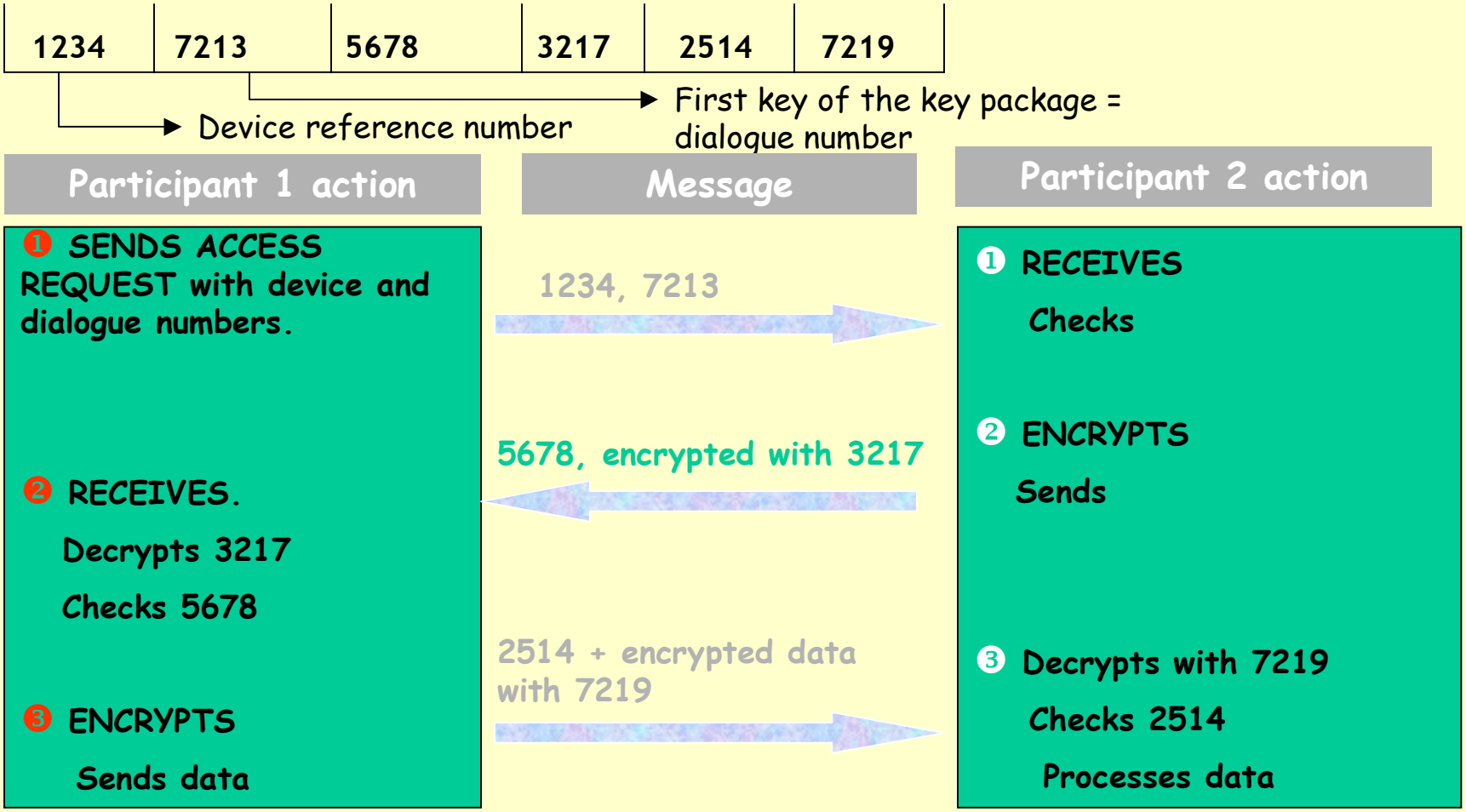
1. Example of dialogue with key interchange and possible application in all types of non-presential operations.

Note: the dialogue number in the example is the 1st key of the key package



2. Example of dialogue with encryption for internet operations.

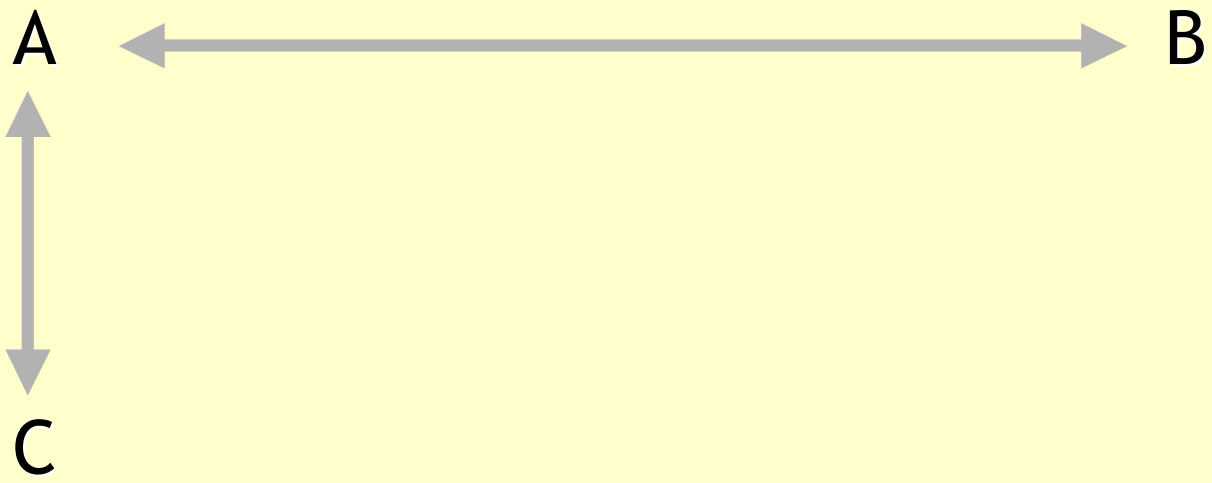
Example of dialogue between two participants, 1 and 2, using the key PACKAGE:



3. Example of dialogue between three participants for an internet operation with authentication.

ONE SOLUTION

Dialogue is broken down into two dialogues, similar the ones in example number 2.



Where A also plays the role of Validation and Intermediation Entity for this operation developed under the authentication procedure.

DIVERSID AUTENTICACIÓN

System Summary 1/2

- Keys are made up of randomly obtained numbers.

- Each message interchanged in the process of an operation can be associated to a different key, which validates such message for the receiver.

- Each message can be encrypted using a different key.

- Each operation uses a key package and, once it is used, will be marked to avoid reutilization

- Authentication process does not consider the called party as identified until the correct key, according to the key package used, is received from the called side

System Summary 2/2

- As the system does not use any temporary variables, there is no limitation for the response time to the messages making up the dialogue.

- It protects the users' identity and sensitive information, allowing encryption.

- One of the set of keys used for the dialogues is stored in a non-accessible pocket size device. The other set resides in a secure system that must support and apply the necessary security procedures to prevent access (secure servers).

Authentication system applications

- Secure access to the internet and intranet
- Internet shopping and payments
- Payment at stores
- ATM operations
- Phone banking
- Mobile phone operations
- Authenticated e-mail
- Domotics