E-Ticketing scheme for mobile devices with exculpability

Arnau Vives-Guasch[1], Magdalena Payeras-Capella[2], Macià Mut-Puigserver[2] and Jordi Castellà-Roca[1]

[1]Dept. de Ingeniería Informática y Matemáticas
Universitat Rovira i Virgili, Spain
email: {arnau.vives, jordi.castella}@urv.cat

[2]Dept. de Ciencias Matemáticas e Informática
Universitat de les Illes Balears, Spain
email: {mpayeras, macia.mut}@uib.es

Data Privacy Management - 5th International Workshop
Athens, Greece. September 23, 2010

Electronic ticket

An **electronic ticket** is a contract, in digital format, between the user and the service provider.

- **Information technologies** (IT) are becoming usual in our society as they progressively replace the use of paper in many of our common operations.
- IT help to **reduce both economic costs and time** in many services such as air **travel industries** or **public transport**.
- The **security** of the system has to be strongly guaranteed, as well as the **privacy** of their users.
- Traditionally, **smart-cards** have been widely used in these systems. Nowadays, **mobile devices** are becoming more increasingly used.

- Authenticity
- Non-repudiation
- Integrity
- Expiry date
- Reusability
- Anonymity
- Online/Offline

Exculpability

The service provider can not falsely accuse the user of ticket overspending, and the user is able to demonstrate that she has already validated the ticket before using it.

Smart-card based proposals

- Smart-card-based proposals [3, 5, 9, 8, 10, 14, 13] establish a communication channel with the verification system for the most sensitive operations.
- The smart-card verifies each operation, so that users can not perform any non-allowed action: considered **tamper-proof** devices.

Non-smart-card based proposals

- Non-smart-card-based systems [11, 4, 1, 6, 12, 7, 2] allow to perform applications with high computation requirements, offering high storage capacity and wireless short-range communication resources.
- High-level cryptographic protection is needed in order to assure the protocol is correctly executed: considered **non-tamper-proof** devices.
  - Non-Anonymous: [4, 1]
  - Revocable-Anonymous: [11, 6, 12, 7, 2]

We present an e-ticketing system that:

- Provides **revocable anonymity** to users
- Introduces **exculpability** as a security requirement
  - Use of crossed one-way collision-resistant hash functions.
- Only one provider is able to give a certain service (for simplicity): **offline** verification.
- Is designed for its application with **mobile devices** for users
  - Reduce computation requirements in the user side

User ($\mathcal{U}$)

Pays for the ticket and receives the service.

Service provider ($\mathcal{P}$)

Gives the service to $\mathcal{U}$.

Ticket issuer ($\mathcal{I}$)

Sends a valid ticket to $\mathcal{U}$ in order to further receive the according service.

Trusted Third Party ($\mathcal{T}$)

Preserves $\mathcal{U}$'s anonymity, and also gives a valid non-identity-linkable pseudonym to $\mathcal{U}$.

- Authenticity
- Non-repudiation
- Integrity
- Expiry date
- Non-overspending
- Revocable Anonymity
- Offline verification
- Exculpability

Ticket Information (T)			
Serial number	Sn	Issuer	Is
Service	Sv	Terms and conditions	Tc
User pseudonym	$\text{Pseu}_{\mathcal{U}}$	Attributes	At
Type of ticket	Ty	Encrypted verification data	$\delta_{\mathcal{T},\mathcal{P}}$
Validity time	Tv	Date of issue	Ti
Exculpability ($\mathcal{U}$)	$\text{h}_{\text{r}_{\mathcal{U}}}$	Exculpability ($\mathcal{P}$)	$\text{h}_{\text{r}_{\mathcal{I}}}$
Digital signature of $\mathcal{I}$	$\text{Sign}_{\mathcal{I}}(\text{T})$		

Receipt Information (R)			
Encrypted exculpability ($\mathcal{P}$)	$\text{A}_{\mathcal{P}}$	Timestamp	τ_i
Ticket serial number	T.Sn	Digital signature of $\mathcal{P}$	$\text{Sign}_{\mathcal{P}}(\text{R})$

Pseudonym Renewal

$\mathcal{U}$ obtains a new temporal pseudonym from $\mathcal{T}$ to be used in the system without linkage to user's identity (if user behaves correctly).

Ticket Purchase

$\mathcal{U}$ pays for the service and receives the ticket from the ticket issuer $\mathcal{I}$.

Ticket Verification

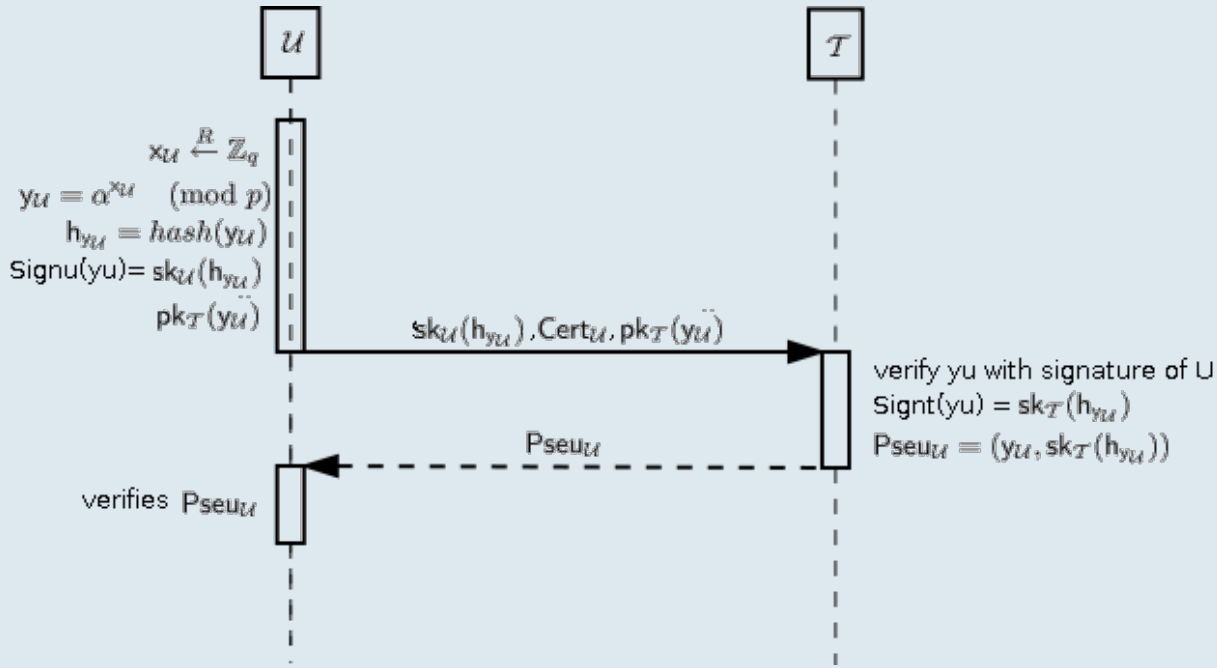
$\mathcal{U}$ shows the ticket to the service provider $\mathcal{P}$ in order to verify that ticket and receive the service.

Claims

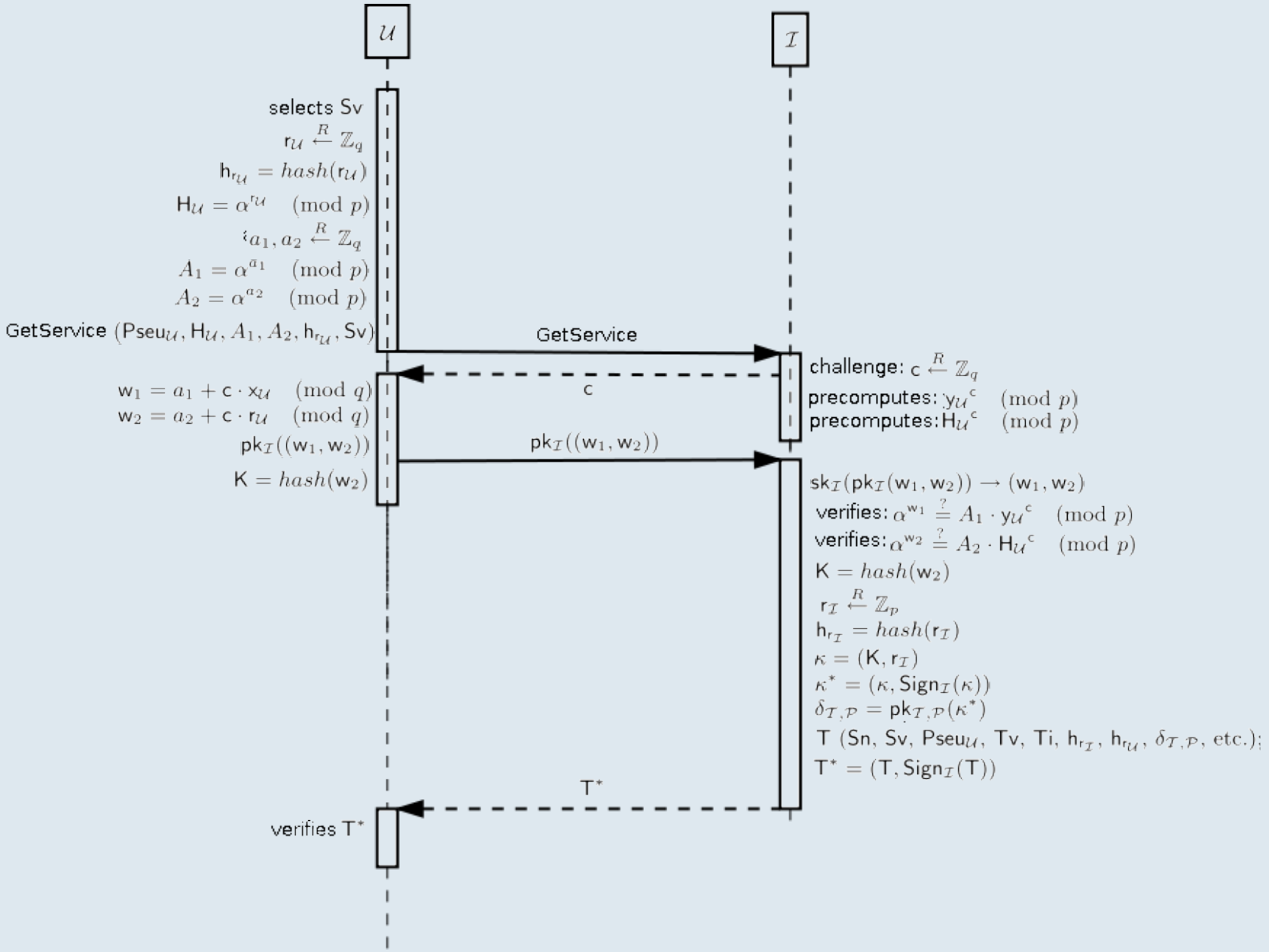
Dispute resolution protocols in case of misbehaviour of any actor to preserve system security. They can contact the TTP $\mathcal{T}$ with:

- Claim m_2 Not Received (m_2: Ticket acceptance by $\mathcal{P}$)
- Claim m_3 Not Received (m_3: $\mathcal{U}$'s exculpability proof)
- Claim m_4 Not Received (m_4: $\mathcal{P}$'s exculpability proof (Receipt))

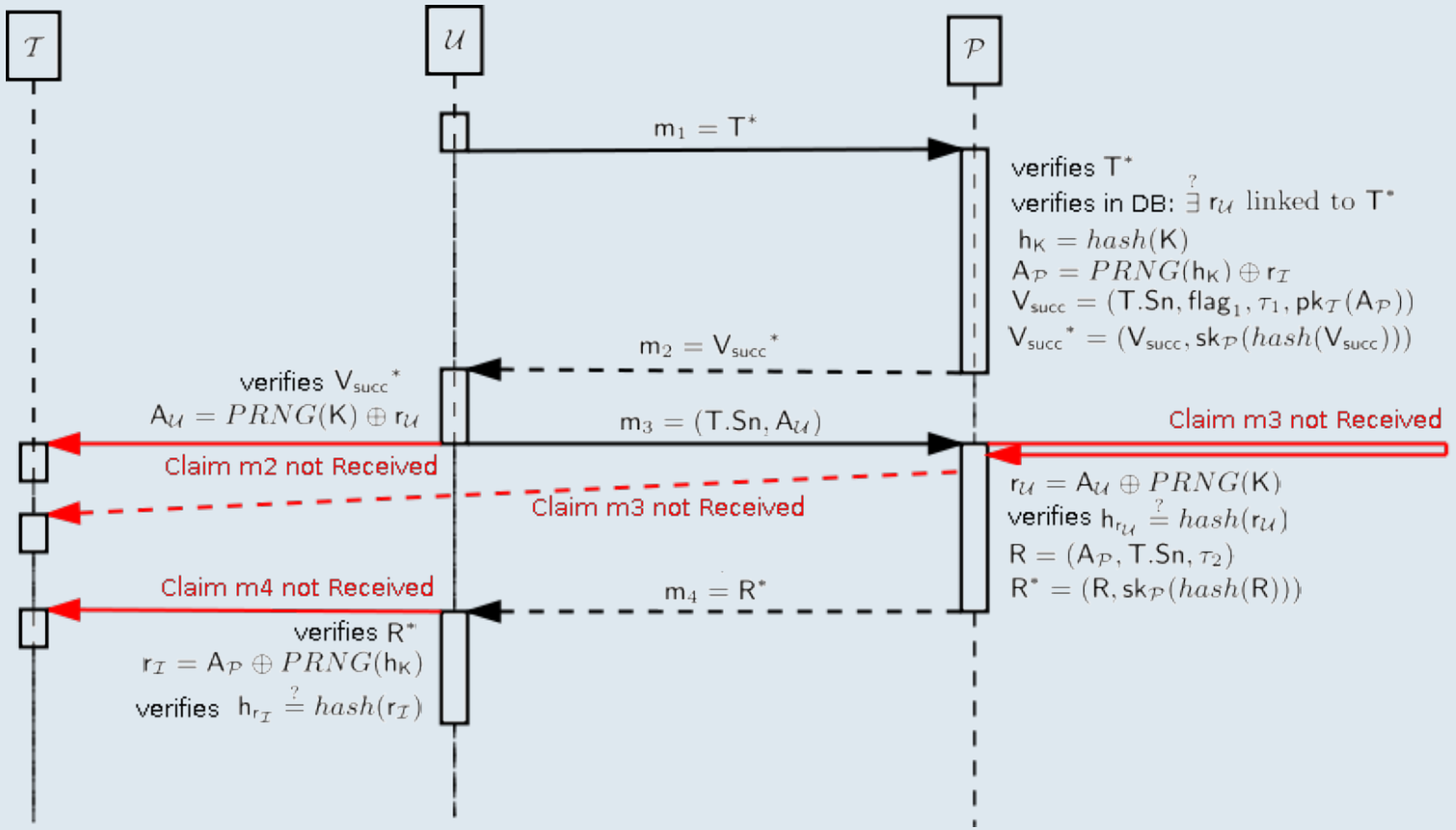
Pseudonym Renewal



Ticket Purchase



Ticket Verification



Claim m_2 not Received (m_2: Ticket acceptance by $\mathcal{P}$)

- $\mathcal{U}$ can contact $\mathcal{T}$ if m_1 has been sent and m_2 has not been received from $\mathcal{P}$
- $\mathcal{U}$ sends the m_1 to $\mathcal{T}$. If valid, $\mathcal{T}$ signs the information with a timestamp and gives the proof to $\mathcal{U}$ and $\mathcal{P}$.
- $\mathcal{P}$ is requested to follow the protocol.

Claim m_3 not Received (m_3: $\mathcal{U}$'s exculpability proof)

- $\mathcal{P}$ blocks till the reception of m_3 by $\mathcal{U}$.
- $\mathcal{P}$ could contact $\mathcal{T}$ if $\mathcal{U}$ repeatedly misbehaves.

Claim m_4 not Received (m_4: $\mathcal{P}$'s exculpability proof (Receipt))

- $\mathcal{U}$ can contact $\mathcal{T}$ if m_3 has been sent and m_4 has not been received from $\mathcal{P}$
- $\mathcal{U}$ sends (m_1, m_2, m_3) to $\mathcal{T}$. If valid, $\mathcal{T}$ signs the information with $(A_{\mathcal{U}}, A_{\mathcal{P}})$ and a timestamp and gives the proof to $\mathcal{U}$.
- $\mathcal{U}$ can obtain the $r_{\mathcal{I}}$.

Multiple providers

- Multiple providers could give the same service with the ticket.
- Online verification between all the providers to avoid ticket overspending.
- Special care to the distribution and control of used tickets (existence of $r_{\mathcal{U}}$ in a central DB).
- Expired tickets removed from the database for storage efficiency.

System security

In the security analysis of the paper, we detail how the security requirements have been achieved: **authenticity**, **non-repudiation**, **integrity**, **expiry date**, **non-overspending**, **offline** verification, and also **exculpability**.

Users' privacy

In the security analysis of the paper, we detail how the **revocable anonymity** has been achieved for honest users by using temporal pseudonyms.

Conclusions

We have presented an e-ticketing scheme with **revocable anonymity**, and **exculpability** as a novel security requirement.

- Use of personal mobile devices.
- Only one provider is able to give a certain service: offline verification.

Further work

- Develop a prototype for mobile devices with short-range contactless communication *(Near Field Communication)*.

E-Ticketing scheme for mobile devices with exculpability

Arnau Vives-Guasch[1], Magdalena Payeras-Capella[2], Macià Mut-Puigserver[2] and Jordi Castellà-Roca[1]

[1]Dept. de Ingeniería Informática y Matemáticas
Universitat Rovira i Virgili, Spain
email: {arnau.vives, jordi.castella}@urv.cat

[2]Dept. de Ciencias Matemáticas e Informática
Universitat de les Illes Balears, Spain
email: {mpayeras, macia.mut}@uib.es

Data Privacy Management - 5th International Workshop
Athens, Greece. September 23, 2010

- F. Bao.
  A scheme of digital ticket for personal trusted device.
  15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC04), 4:3065–3069, 2004.
  IEEE.
- Yu-Yi Chen, Chin-Ling Chen, and Jinn-Ke Jan.
  A mobile ticket system based on personal trusted device.
  Wireless Personal Communications: An International Journal, 40(4):569–578, 2007.
- J. Elliot.
  The one-card trick multi-application smart card e-commerce prototypes.
  Computing & Control Engineering Journal, 10(3):121–128, 1999.
  IET.
- K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno, and J. Sekine.
  Digital-ticket-controlled digital ticket circulation.
  8th USENIX Security Symposium, pages 229–240, 1999.
  USENIX.
- D. Haneberg.
  Electronic ticketing: risks in e-commerce applications.
  Digital excellence, pages 55–66, 2008.
  Springer-Verlag, ISBN 3540726209.
- Dominik Haneberg, Kurt Stenzel, and Wolfgang Reif.
  Electronic-onboard-ticketing: Software challenges of an state-of-the-art m-commerce application.
  In K.Pousttchi and K.Turowski, editors, *Workshop Mobile Commerce*, volume 42 of *Lecture Notes in Informatics (LNI)*, pages 103–113.
  Gesellschaft für Informatik (GI), 2004.
- Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu.
  Privacy for public transportation.
  In *6th Workshop on Privacy Enhancing Technologies (PET 2006)*, pages 1–19, 2006.
  LNCS 4258.
- K. Kuramitsu and K. Sakamura.
  Electronic tickets on contactless smartcard database.
  In *Proceedings of the 13th International Conference on Database and Expert Systems Applications*, pages 392–402, 2002.
  LNCS 2453.
- Kimio Kuramitsu, Tadashi Murakami, Hajime Matsuda, and Ken Sakamura.
  Ttp: Secure acid transfer protocol for electronic ticket between personal tamper-proof devices.
  In *24th Annual International Computer Software and Applications Conference (COMPSAC2000)*, pages 87–92, Taipei, Taiwan, Oct 2000.
  vol. 24.
- S. Matsuo and W. Ogata.
  Electronic ticket scheme for its.