University of the Aegean

De Facto Joint Research Group

Certificate Revocation: What Is It and What Should It Be

John Iliadis[1,2], Stefanos Gritzalis[1]

[1]Department of Information and Communication Systems Engineering
University of the Aegean
E-mail: {jiliad,sgritz}@aegean.gr

[2]Department of Informatics
Technological Educational Institute of Athens
E-mail: jiliad@cs.teiath.gr

Overview

- Introduction
- What is Certificate Revocation ?
- Proposed mechanisms for Certificate Status Information
- Evaluation criteria for CSI mechanisms
- The need for an alternative mechanism
- Alternative Dissemination of CSI (ADoCSI)
- Problems to be solved in ADoCSI

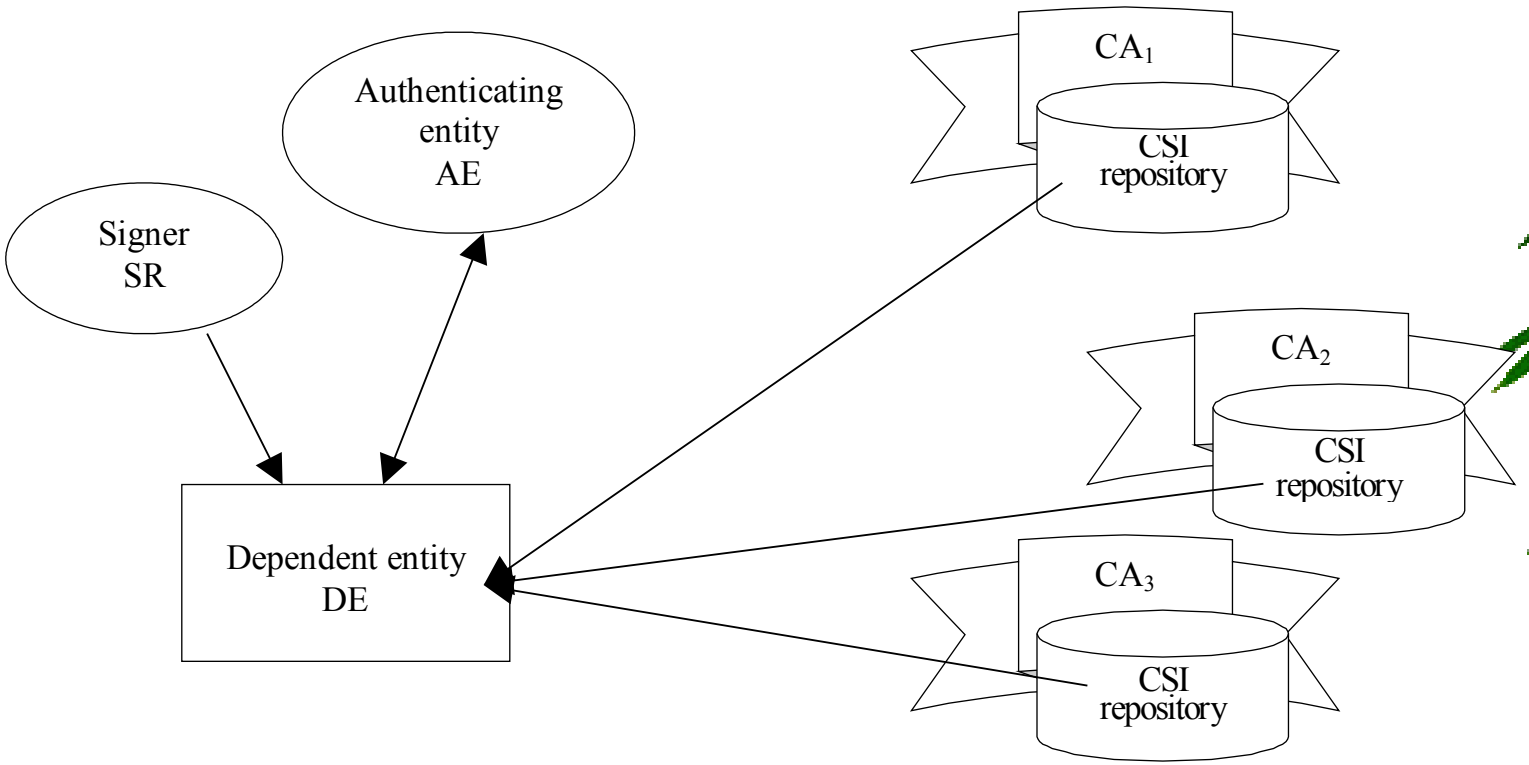
John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Introduction

1. Is PKI a new era for Network Security?
2. Certificate Revocation? What Certificate Revocation?
3. Certificate Status Information Mechanisms
4. EU Directive: “secure and prompt revocation service”

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Certificate Revocation



John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

CSI Mechanisms: CRLs

- Certificate Revocation Lists
- Compare to Black lists: Banks, Cell phone Operators. Dependent entities: merchants (online POS), Banks, other Cell phone operators
- CRL: Signed list containing serial numbers of revoked (/suspended?) certificates, the revocation dates and (optional) reasons

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

CSI Mechanisms: CRLs (cont.)

- Delta-Certificate Revocation Lists
- Distribution Points
- Fresh Revocation Information (DeltaCRLs on top of DP CRLs)
- Redirect CRL (dynamic re-partitioning of large DP CRLs)

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

CSI Mechanisms: (cont.)

- Enhanced CRL Distribution Options
  - Separate location and validation functions.
- Positive CSI
  - CRLs are all wrong… CSI should contain positive, not negative info. Dependent entity should set ad hoc freshness requirements and certificate holder should provide ad hoc CSI.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

CSI Mechanisms: (cont.)

Online Certificate Status Protocol

- Server returning signed CSI corresponding to CSI requests by dependent entities. Possible OCSP Responses:
  1. “Good”, meaning certificate has not been revoked,
  2. “Revoked”, meaning certificate has been revoked or suspended,
  3. “Unknown”, OCSP is not aware of that certificate

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

CSI: Freshness-constrained Revocation Authority

- Repositories of CSI need not be trusted
- Separation of Certification Authority and Authority that issues CSI (Revocation Authority, RevA)
- Dependent entity requires fresh enough CSI from certificate holder

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Evaluation Criteria: Type of Mechanism

- M1: Transparency,
- M2: Offline revocation,
- M3: Delegation of revocation,
- M4: Delegation of CSI dissemination,
- M5: Delegation of certificate path validation,
- M6: Referral capability,
- M7: Revocation reasons.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Evaluation Criteria: Efficiency

- E1: Timeliness of CSI,
- E2: Freshness of CSI,
- E3: Bounded revocation,
- E4: Emergency CSI capability,
- E5: Economy,
- E6: Scalability,
- E7: Adjustability.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

Evaluation Criteria: Security

- S1: CSI disseminator authentication,
- S2: CSI integrity,
- S3: CA compromise
- S4: RevA compromise,
- S5: Contained functionality,
- S6: Availability.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

The need for an alternative CSI mechanism

- Dependent entities and certificate holders are not necessarily experienced computer-users, nor are they security aware,
- PKI security-related procedures have to be made more transparent, as in the credit card system.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

An Agent-based mechanism

- The transparency criterion has to be met: location, retrieval and validation of CSI has to be made transparent to the dependent entity.
- An Agent-based mechanism could do that, using the aforementioned CSI mechanisms and providing an indirection layer between dependent entity and CSI mechanisms

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

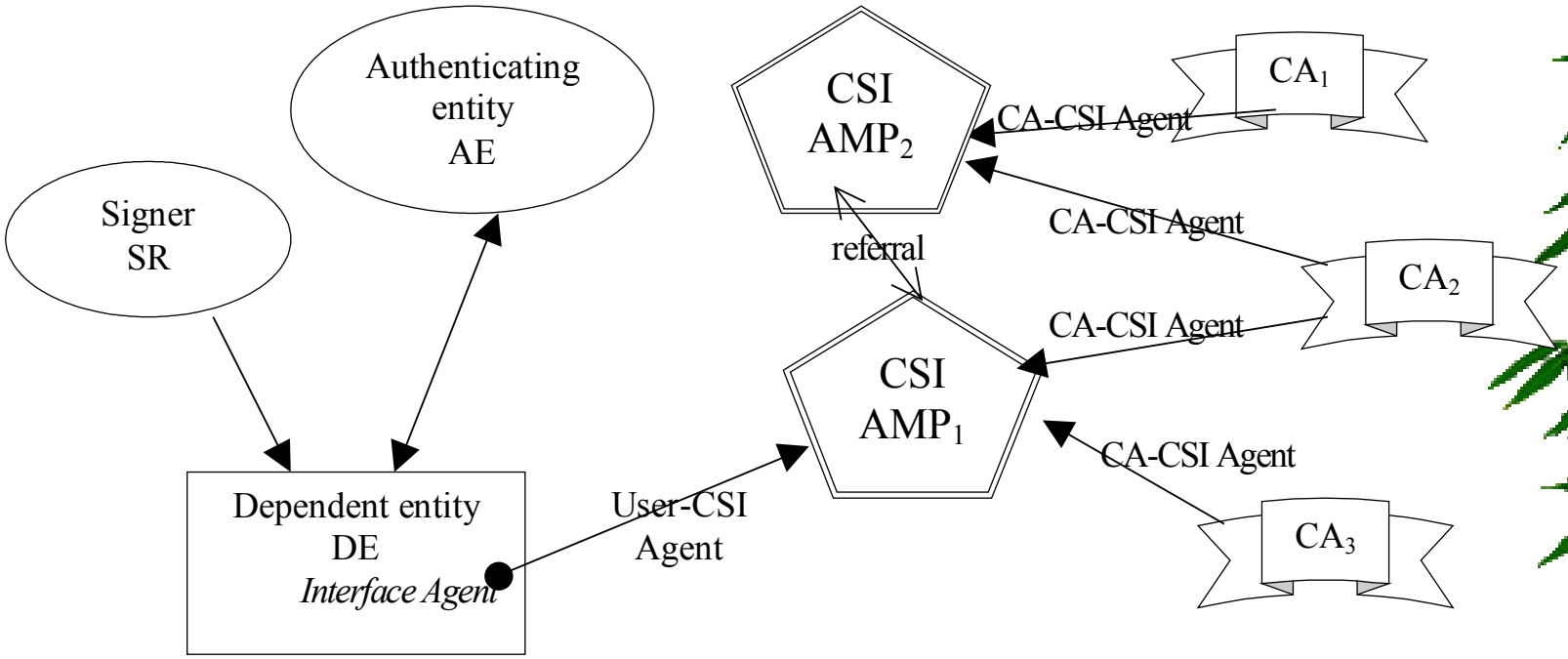
ADoCSI: Alternative Dissemination of Certificate Status Information

The agents ADoCSI needs must be able to:

1. Suspend execution and resume it at another execution environment,
2. Retain their state, when transporting themselves to other execution environments,
3. Create child agents and deploy them,
4. Select a network location, out of a list of locations, with the least network congestion,
5. Communicate the retrieved information back to their owner or to their owner's application that spawned the agent.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

ADoCSI



John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

ADoCSI (2)

1. Agent Meeting Places (AMP) (also called Agent Platforms)
2. Dependent entity,
3. Authenticating Entity or Signer,
4. Certification Authority Certificate Status Information (CA-CSI) Agent,
5. User Certificate Status Information (User-CSI) Agent,
6. Interface Agent.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

ADoCSI: Problems seeking solutions

ADOCSI researchers must find solutions to a series of problems that emerge from using Agents in CSI, namely :

2. How can the location function be implemented transparently ?
3. How can dependent entities retrieve and validate CSI transparently ?
4. How is a certificate path validated ?
5. What is the way this mechanism interacts with dependent entities ?
6. How are Agents protected from unauthorised modification or replacement ?
7. How can CSI carried by Agents be protected ?
8. How can an Agent tell a fraudulent Agent Meeting Place ?

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

ADoCSI: Problems seeking solutions (2)

1. How can AMPs be protected from DoS attacks ?
2. How can dependent entities be protected against User-CSI Agent replay attacks ?
3. How are the Agent Meeting Places protected from malicious Agents ?
4. How can an Agent retrieve CSI for a dependent entity, without letting the AMP know which certificate did it retrieve CSI for ?

A first paper commenting on these issues will soon appear.

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

References

- References of general interest (PKI mostly)
- References to certificate revocation resources
- References to papers on securing Software Agents

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002

References (2)

- References of general interest (PKI mostly)
- References to certificate revocation resources
- References to papers on securing Software Agents

John Iliadis, Stefanos Gritzalis
University of the Aegean, IPICS 2002