ADoCSI: Towards a Transparent Mechanism for Disseminating Certificate Status Information

John Iliadis, PhD student
Dept. of Information and Communication Systems Engineering
University of the Aegean
E-mail: jiliad@aegean.gr

Overview

- What is Certificate Revocation ?
- 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

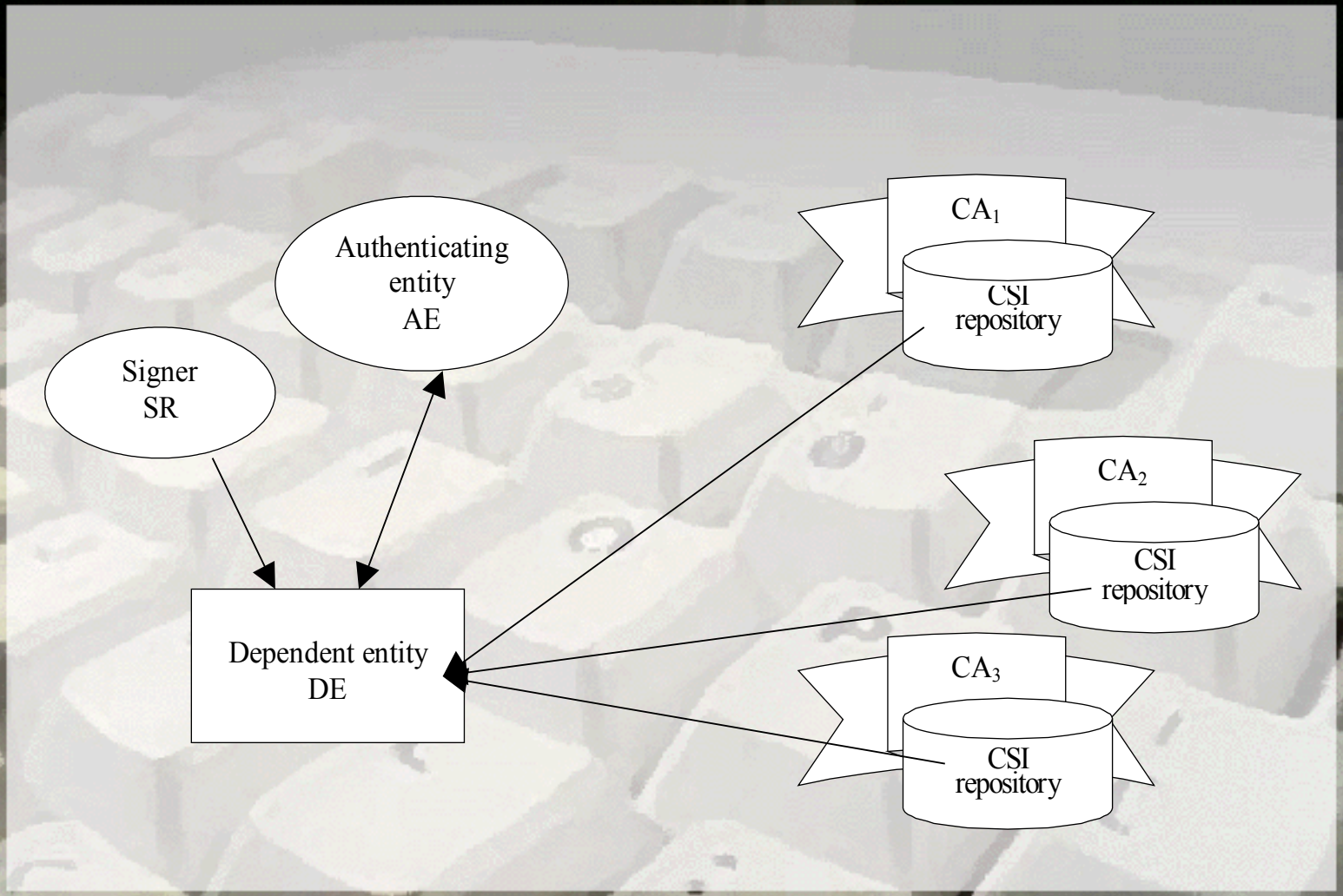
Introduction

2. Certificate Revocation? What Certificate Revocation?

4. Certificate Status Information Mechanisms

6. EU Directive: “secure and prompt revocation service”

Certificate Revocation



CSI Mechanisms: 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

CSI Mechanisms: Certificate Revocation Lists (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)

CSI Mechanisms: Certificate Revocation Lists (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.

CSI Mechanisms: 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 “Good”, meaning certificate has not been revoked,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 “Revoked”, meaning certificate has been revoked or suspended,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

CSI Mechanisms: 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

Evaluation Criteria: Type of Mechanism

- Transparency,
- Offline revocation,
- Delegation of revocation,
- Delegation of CSI dissemination,
- Delegation of certificate path validation,
- Referral capability,
- Revocation reasons.

Evaluation Criteria: Efficiency

- Timeliness of CSI,
- Freshness of CSI,
- Bounded revocation,
- Emergency CSI capability,
- Economy,
- Scalability,
- Adjustability.

Evaluation Criteria: Security

- CSI disseminator authentication,
- CSI integrity,
- CA compromise
- RevA compromise,
- Contained functionality,
- Availability.

The need for an alternative CSI mechanism

- Dependent entities and certificate holders:
  - experienced computer-users ?
  - security aware ?
- PKI security-related procedures have to be made more transparent (e.g. bank cards)

An Agent-based mechanism

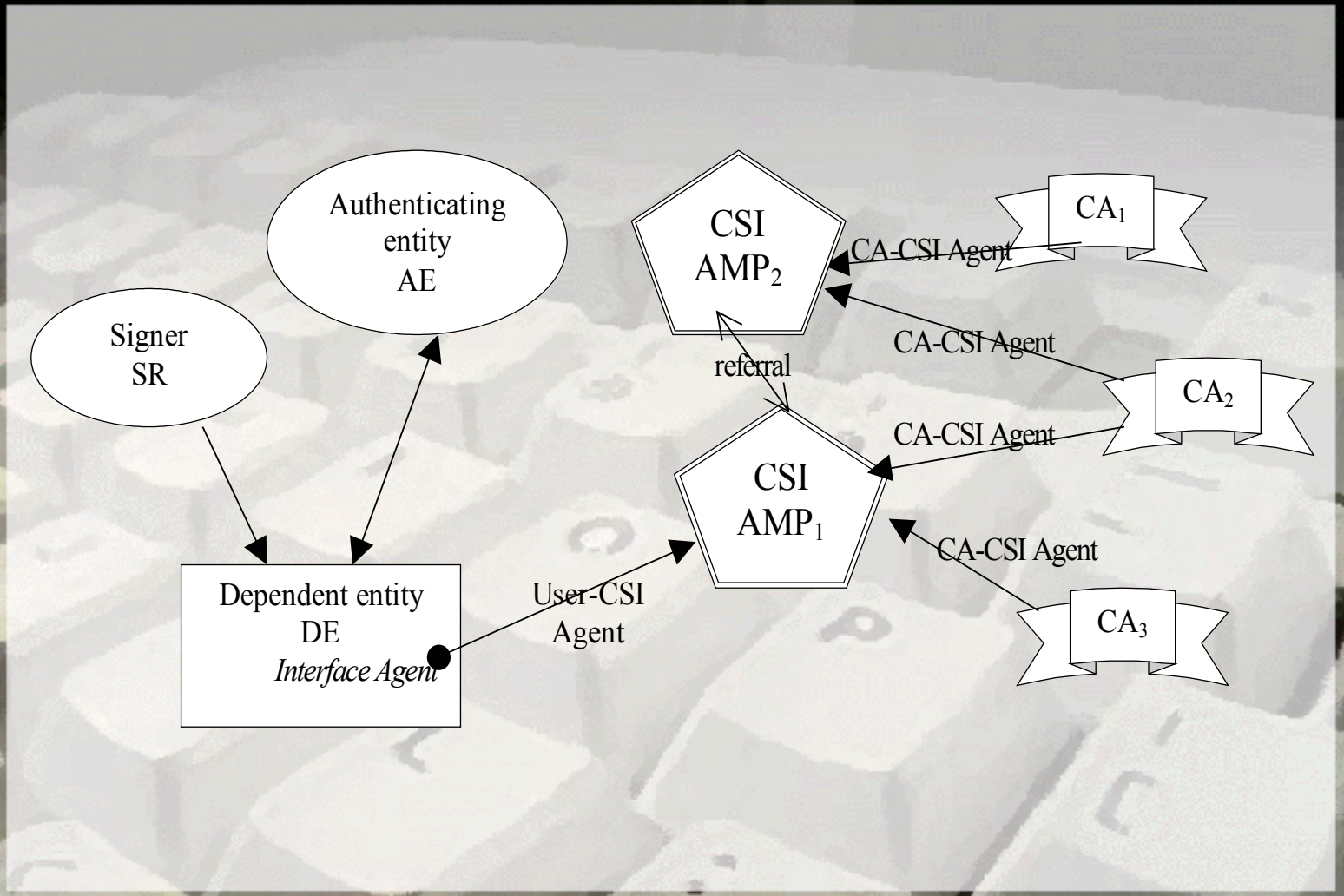
- The transparency criterion has to be met:
  - *Transparently locating CSI*
  - *Transparently retrieving CSI*
  - *Transparently validating CSI*
- Agent-based mechanism
  - *using existing CSI mechanisms*
  - *providing an indirection layer between dependent entity and CSI mechanisms*

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.

ADoCSI: Alternative Dissemination of Certificate Status Information



ADoCSI Recipe Ingredients

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.

ADoCSI: Problems seeking solutions

1. How can the location function be implemented transparently ?

3. How can dependent entities retrieve and validate CSI transparently ?

5. How is a certificate path validated ?

7. What is the way this mechanism interacts with dependent entities ?

ADoCSI: Problems seeking solutions (2)

1. How are Agents protected from unauthorised modification or replacement ?

3. How can CSI carried by Agents be protected ?

5. How can an Agent tell a fraudulent Agent Meeting Place ?

7. How can AMPs be protected from DoS attacks ?

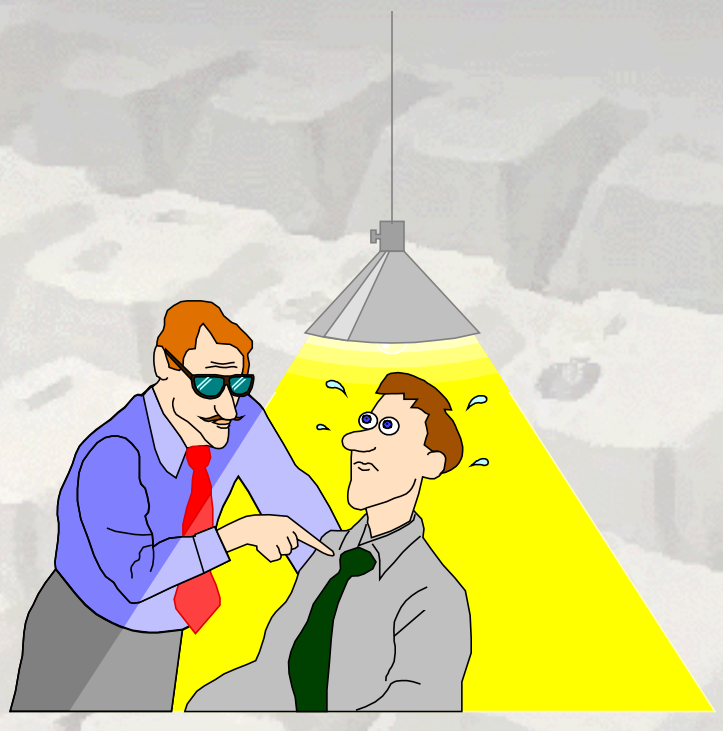
ADoCSI: Problems seeking solutions (8)

1. How can dependent entities be protected against User-CSI Agent replay attacks?

3. How are the Agent Meeting Places protected from malicious Agents ?

5. How can an Agent retrieve CSI for a dependent entity, without letting the AMP know which certificate did it retrieve CSI for ?

Q&A

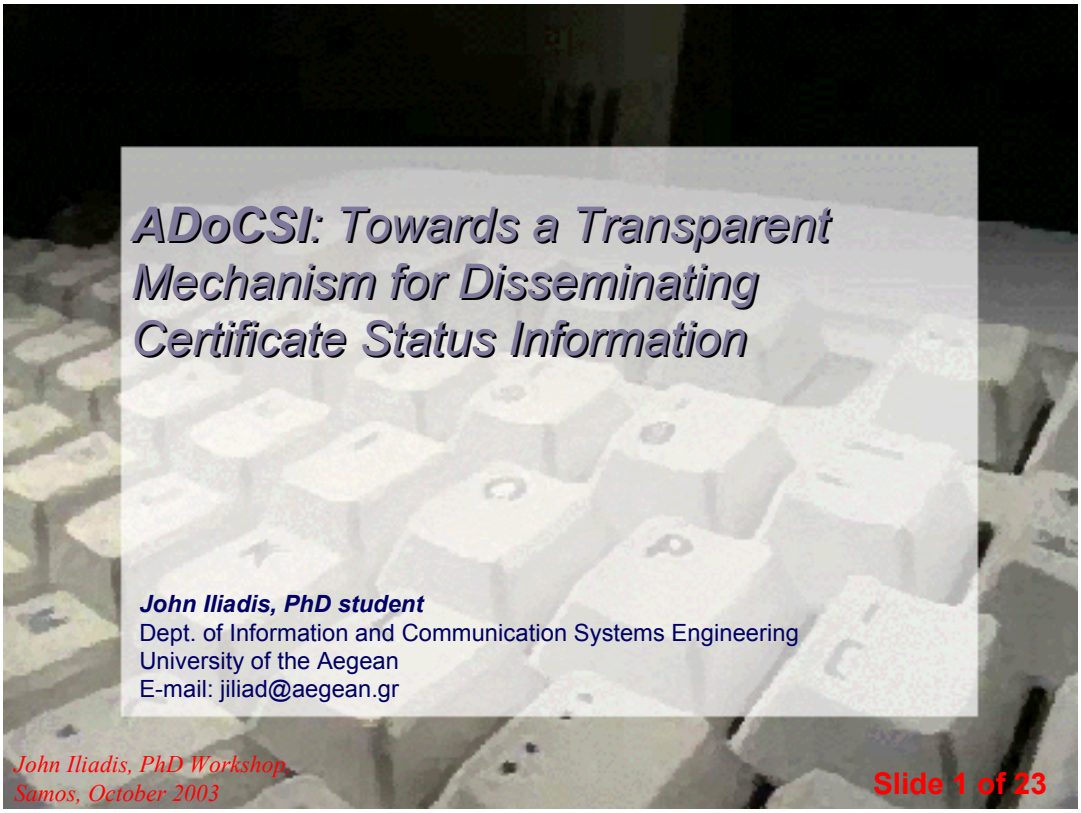


References

- PKI
- Certificate Revocation
- Software Agents' Security

References (2)

- PKI
- Certificate Revocation
- Software Agents' Security

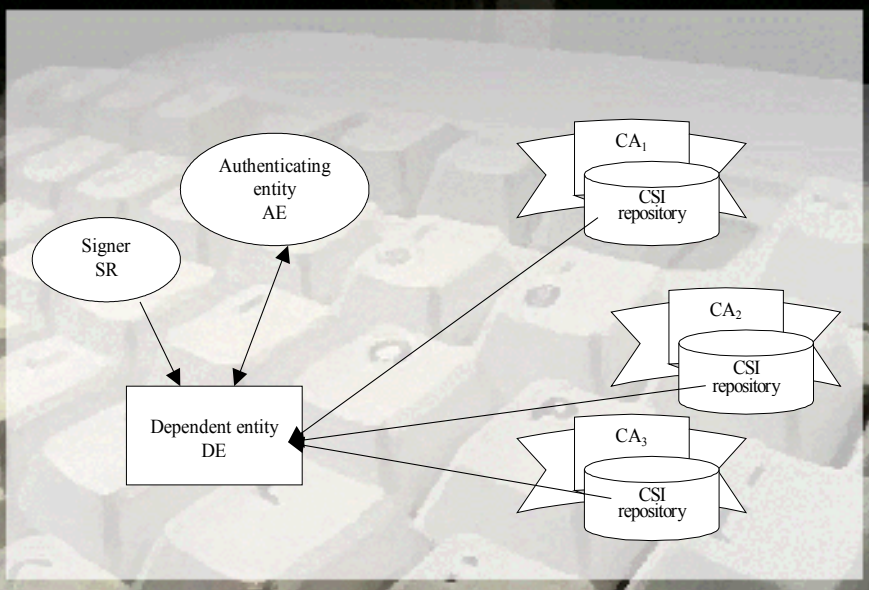

ADoCSI: Towards a Transparent Mechanism for Disseminating Certificate Status Information
John Iliadis, PhD student
Dept. of Information and Communication Systems Engineering
University of the Aegean
E-mail: jiliad@aegean.gr
John Iliadis, PhD Workshop, Samos, October 2003
Slide 1 of 23

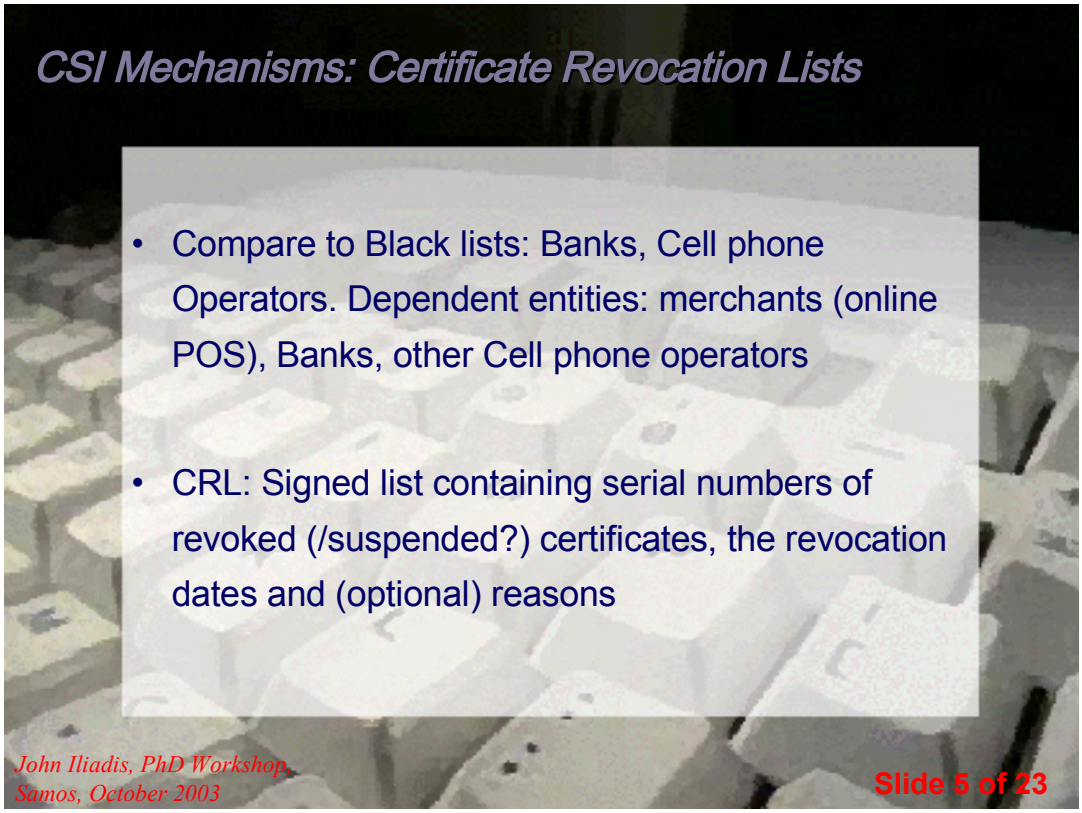

Overview
• What is Certificate Revocation ?
• Mechanisms for Certificate Status Information
• Evaluation criteria for CSI mechanisms
• The need for an alternative mechanism
• Alternative Dissemination of CSI (ADoCSI)
• Problems to be solved in ADoCSI
John Iliadis, PhD Workshop, Samos, October 2003
Slide 2 of 23

Although laws have already been voted, and regulatory frameworks put in place, PKI is being expanding without this extra care needed for revocation. Both technical and legal requirements exist (e.g. EU Directive "secure and prompt revocation service). However, certificate holders and dependent entities have not yet realised the need for it.

Government seems to be the driving force for PKI; at least in Europe, e-gov initiatives do/could take advantage of PKI. User awareness programmes could be initiated by appropriate government actions.

Certificate Revocation





Certificate Revocation Lists Standards: X.509, ISO 9594, RFC 2459

A dependent entity has to locate, retrieve and validate a CRL. The location function can be embedded in the certificate of the signer.

•Can/will the s/w the dependent entity uses retrieve and validate the CRL?

•If CRL not found or old, must the s/w attempt to locate a more recent version or alert the dependent entity?

•Is the dependent entity security-aware? What about authentication fatigue?

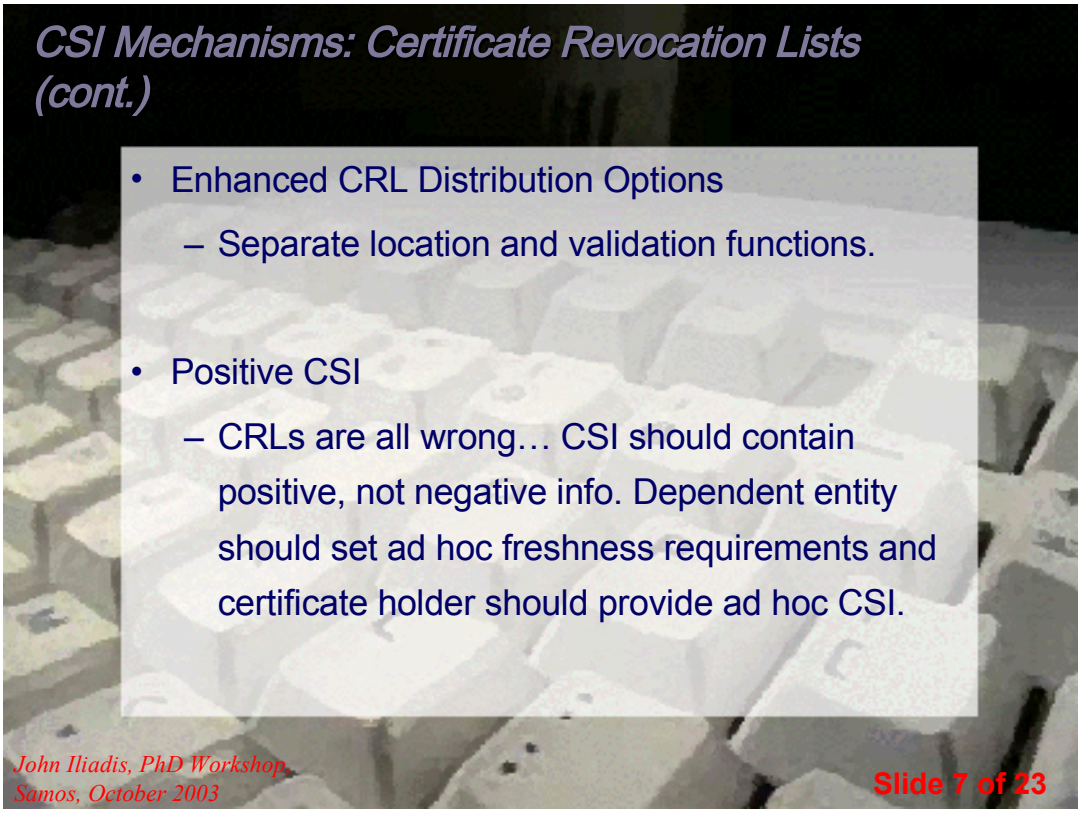
•How can a dependent entity validate a CRL if it does not possess the certificate used to sign it, or the CA certificate ?

•Delta-CRL: Containing only the changes/additions since the last full CRL (DeltaCRLIndicator extension)

•Distribution Points: Partitioning of CRLs depending on: certificate serial numbers, namespaces, issuance dates, …

•Fresh Revocation Information: DeltaCRLs on top of DP CRLs

•Redirect CRLs: Dynamic re-partitioning of CRLs when they grow to be unmanageably large. Extension in DP CRL, pointing to the new DP CRL.



Location and **Validation** functions in CSI:

The location function is used in order to locate the source of CSI the dependent entity is looking for. It is usually contained in the certificate of the signer.

The validation function is used in order to verify that a retrieved piece of CSI contains status information regarding the certificate presented to the dependent entity by the certificate holder.

Enhanced CRL Distribution Options

According to the Enhanced CRL Distribution Options mechanism, the location and validation functions can be separated in the following way:

Certificate of certificate holder contains a pointer to an empty CRL, which contains only a StatusReferral extension, pointing to newly issued CRLs. The latter contain cRLScope extensions, integrating the validation function.

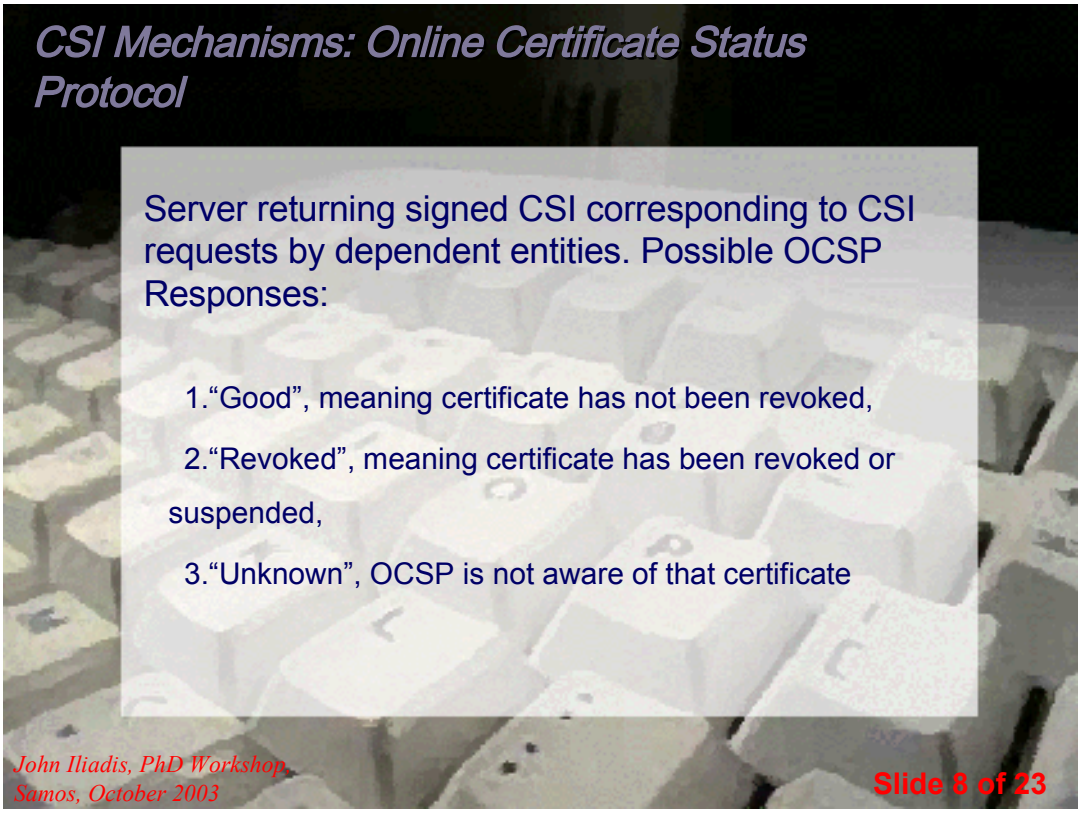
Using Enhanced CRL Dist. Options, a dependent entity needs not download CSI in order to establish whether it is more fresh to the one it already possesses, thanks to StatusReferrals. Moreover, dynamic re-partitioning and load-balancing of CSI can be achieved through cRLScope extensions contained in the actual CRLs.

Positive CSI

According to Positive CSI, it should be the dependent entity that should set freshness requirements for CSI, dynamically and depending on each case where certificates are used. Furthermore, it must be the certificate holder that has to provide the dependent entity with the requested CSI.

A certificate holder should be able to revoke his own key on his own, by signing a “Suicide Note” and delivering it to a “Suicide Bureau”. There should be a network of "Suicide Bureaus" (SB), which gather suicide notes from every possible source, and either replicate the information they hold or have a means to refer queries to each other.

When a dependent entity wishes for CSI it can ask for fresh CSI from the certificate holder; the latter, in turn, should ask an SB for a "certificate of health", stating that ‘no evidence has been received that the key has been lost or compromised’. The dependent entity could set in this case requirements on the freshness of the "certificate of health" provided by the SB to the certificate holder and by the latter to the dependent entity.



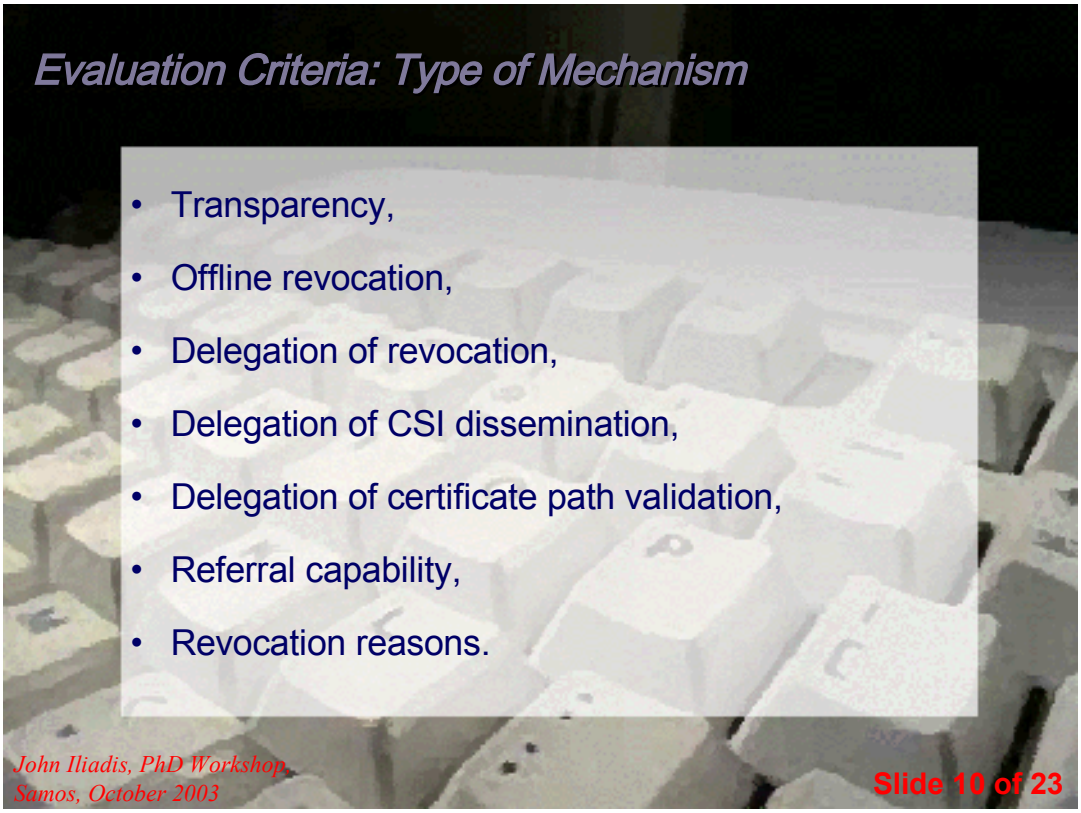
OCSP responses can contain three values concerning time:

1. thisUpdate, which indicates the time at which the CSI communicated to the requester was known to be correct,
2. nextUpdate, which indicates when the next update of CSI is expected to be available,
3. producedAt, which indicates the time at which the CSI communicated to the requester was signed by the entity that runs the OCSP service.

Freshness-constrained Revocation Authority proposes a revocation service where revocation can be definite, and where the repositories of revocation information need not be trusted. According to this service, the role of the Certification Authority (CA) is separated from the role of the Revocation Authority (RevA). The CA issues long-term certificates, which contain freshness constraints on the CSI the dependent entities will use in order to validate the certificates. Such a certificate also contains a pointer to the RevA that is responsible for issuing CSI regarding the specific certificate. The RevA issues frequently timestamped certificates which are used in order to provide the dependent entities with positive assertions regarding the validity of the certificate. The dependent entities themselves impose their own CSI freshness requirements, when certificate holders use their certificates in order to authenticate themselves.

When a certificate holder attempts to authenticate, the dependent entity will impose its own freshness requirements and will expect from the certificate holder to provide a short-lived certificate, issued by the RevA, that fulfils these freshness requirements

It is obvious that this method allows for flexible balancing of the authentication costs and level of protection on a per transaction basis. Furthermore, the CSI, that is the short-lived, timestamped certificate, need not be communicated from a trusted repository. .



M1. Transparency. Transparency in locating the CSI repository (CSI location function) and verifying that the CSI contained in that repository is the one the dependent entity is looking for (CSI validation function),

M2. Offline revocation. Whether a user can revoke his certificate by himself without having to contact the respective CA,

M3. Delegation of revocation. Delegation of the revocation by the CA to another authority, either another CA or another authority that operates only as a Revocation Authority (RevA) and not as a Certification Authority,

M4. Delegation of the CSI dissemination. Delegation of CSI dissemination by the CA to another authority; the latter may be trusted by the dependent entities or not, depending on the mechanics of the CSI dissemination in each case,

M5. Delegation of the certificate path validation. Delegation of the certificate path validation from the dependent entity to another entity; the dependent entity should be provided with the means to verify the origin of the validation result; in addition to that, the entity that performs the certificate path validation should be trusted by the dependent entity,

M6. Referral capability. If the CSI repository does not contain the CSI the dependent entity is looking for, the repository could refer the dependent entity to another CSI repository that may contain the aforementioned CSI,

M7. Revocation Reasons. The certificate path validation function should take into consideration the reasons for the revocation of a certificate (e.g. reasonCode in X.509v2 CRLs) in order to assert on the validity of a certificate in a certificate path.

E1. Timeliness of CSI. Dependent entities should be able to locate and receive CSI on time, for them to use such information in authenticating entities or verifying the signatures of entities,

E2. Freshness of CSI. How 'fresh' is the status information delivered to dependent entities,

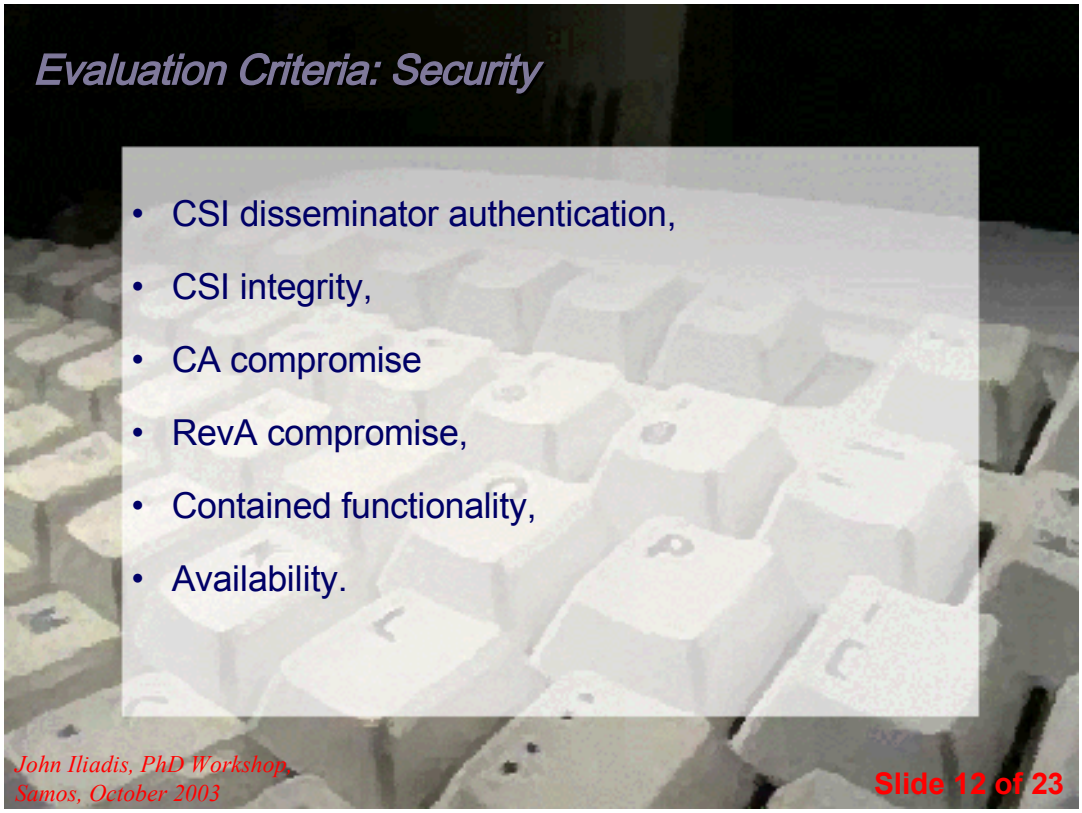
E3. Bounded revocation. New CSI should become available to the dependent entities within a bounded time period,

E4. Emergency CSI capability. Facility to generate emergency CSI to the dependent entities (e.g. in case the certificate of an entity that many people use and trust has been revoked),

E5. Economy. Economy should be examined both from the point of view of the authorities that control the use of certificates (e.g. Certification Authorities, Registration Authorities, Revocation Authorities) and from the point of view of the entities that use certificates (e.g. dependent entities, certificate holders). The CSI dissemination mechanism should not cause any obstacles, delays or disruptions in the normal working practice that the dependent entities and certificate holders follow. The CSI dissemination mechanism should not require from the dependent entities or certificate holders to have a clear and profound understanding of the mechanism itself, and interact to a great extent with the mechanism in order to make it operate properly.

E6. Scalability. When the number of the CSI dissemination mechanism authorities and users (e.g. CAs, RevAs, dependent entities, certificate holders) increases, new problems or difficulties in the operation of the mechanism should not emerge. Scalability relates more to resources, in contrast to economy which relates more to infrastructure and mode of operation,

E7. Adjustability. The dependent entities (or the CA, RevA as well) should be able to adjust the location or validation function operation in order to create a balance between performance and protection, depending on the requirements and the risk policy in each case. Ideally, the dependent entity should be able to do this, since it is the dependent entity that takes the risk.



S1. *CSI disseminator authentication*. Dependent entities must verify the origin of the CSI they receive. The CSI disseminator is usually the RevA (the service is operated by the CA) itself. If authentication is not used, a malicious entity pretending to be a trusted CSI dissemination entity, could provide the dependent entities with false CSI that appears to be valid,

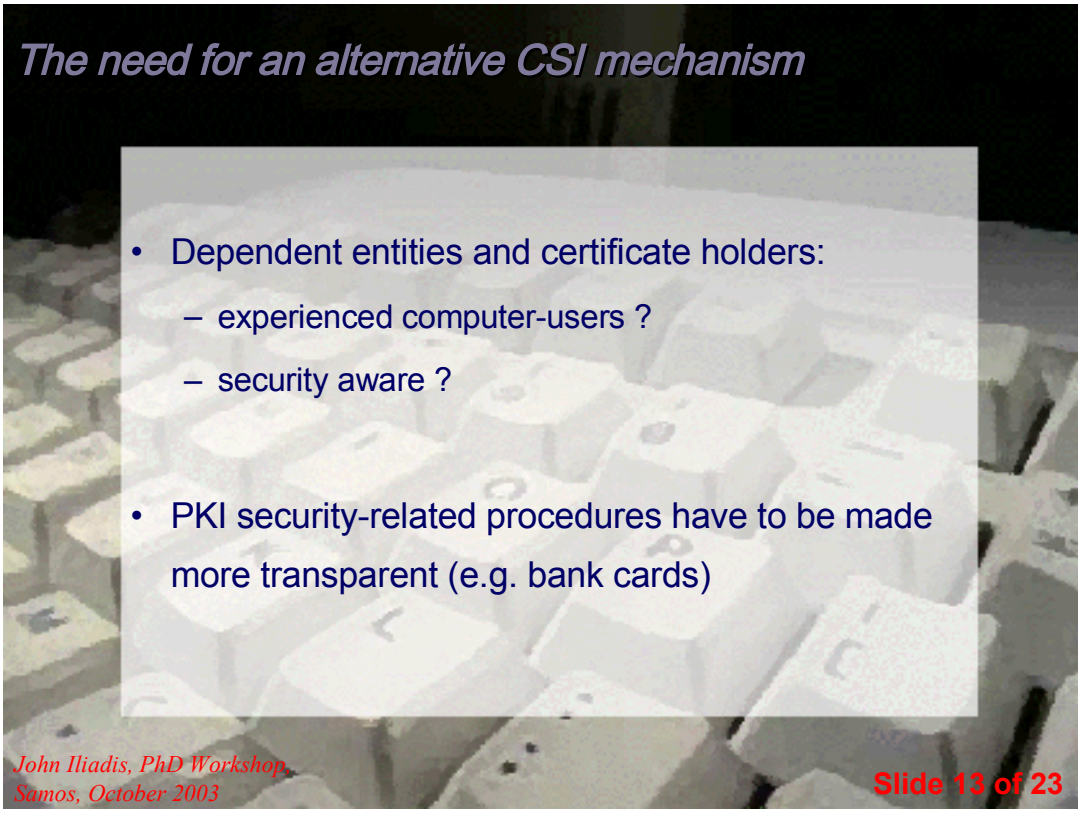
S2. *CSI integrity*. Verifying the integrity of the CSI, when it is stored in the CSI repository, transferred to the dependent entities and when it is stored in the dependent entities' local repository. Such verification must be possible lest a malicious entity modifies the CSI in transit, before the dependent entity receives it; should this happen, the dependent entity may not realise that the received CSI is old, partial or invalid in any way,

S3. *CA compromise*. The effects of a CA key being compromised should be minimised,

S4. *RevA compromise*. There should be a mechanism for the dependent entities to know whether the RevA has been compromised. This mechanism must not be the same with the one used by the dependent entities in order to receive CSI on certificates that belong to entities other than the RevA,

S5. *Contained functionality*. If RevA is compromised, it should not be possible for the entities that gained control of the RevA to issue new certificates,

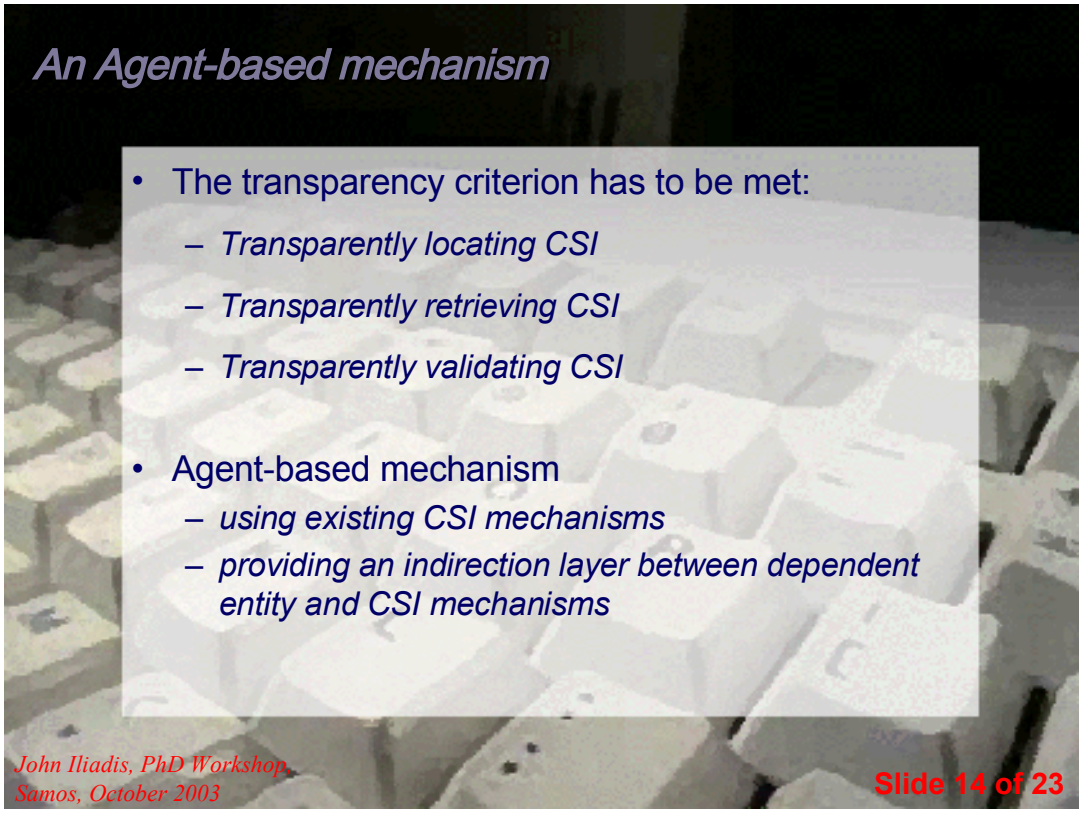
S6. *Availability*. The CSI dissemination mechanism has to be resilient against unreliable networks.



Users are not necessarily experienced computer users; the majority of them are not sensitive or cautious enough about security measures. Even when they are, there are other reasons that could lead them into taking the wrong security decisions, such as “authorisation fatigue”.

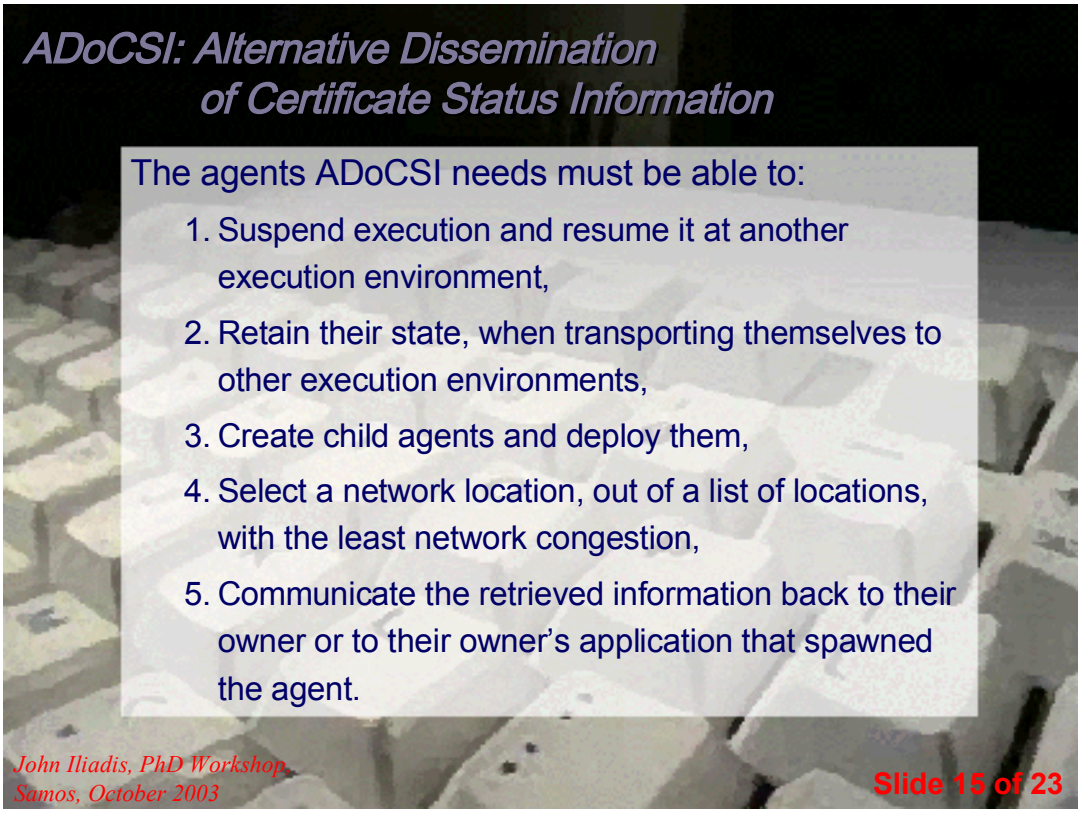
Security-related processes have to be made more transparent, for those users to be able to offer and receive securely electronic services. This is the reason why the use of credit and debit cards has expanded. End-users of the credit and debit card system (cardholders) and the respective dependent entities (e.g. merchants) do not need to take any special security measures in order to take advantage of the credit and debit card system. All they have to do is adopt simple human procedures in order to facilitate the operation of the underlying security system.

This has to be done with PKI as well, in the long run. Authenticating entities, signers and dependent entities should not have to carry out special security procedures. There has to be a security infrastructure that allows them to profit from the use of certificates without them having to contribute to the operation of that security infrastructure, except for some simple procedures which would ensure that the security infrastructure works for their profit.

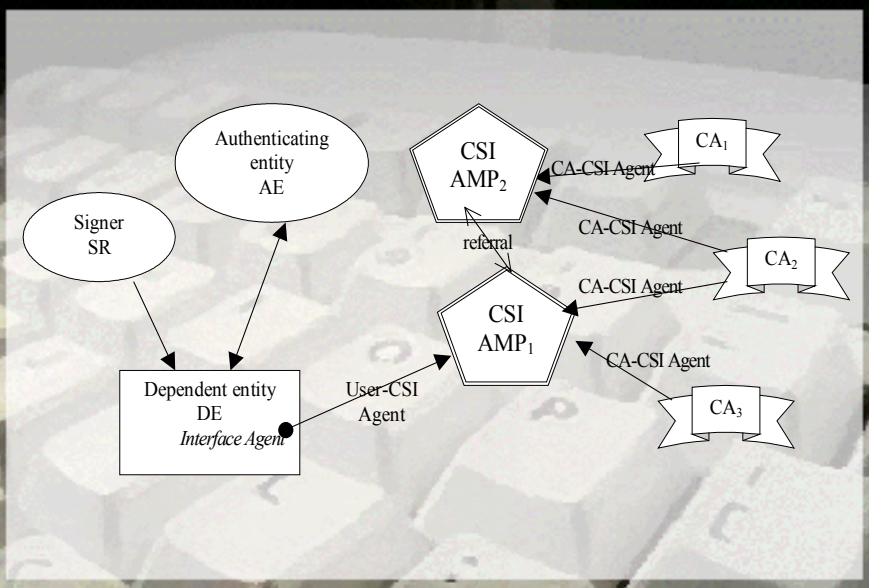


The transparency criterion has to be met, for CSI mechanisms to succeed in the distant future. A level of indirection could be added to them, using Software Agents that carry out the CSI location, retrieval and validation tasks a human would have to do otherwise.

Agents residing in the domain of dependent entities' will decide what CSI the dependent entities need or will need, roam the network in order to locate that CSI and retrieve it for the dependent entities once they are connected again to the network. The major difference of such a mechanism to the others would, or rather should, be transparency. Such a mechanism could use all CSI formats and mechanisms already presented; all the Agent will do is add a level of indirection, thus providing CSI mechanism transparency to the security unaware dependent entity. Such a mechanism is currently under research, at the University of the Aegean. We call it ADOCSI (Alternative Dissemination of Certificate Status Information).


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, PhD Workshop, Samos, October 2003
Slide 15 of 23

ADoCSI: Alternative Dissemination of Certificate Status Information




ADoCSI Recipe Ingredients
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, PhD Workshop, Samos, October 2003
Slide 17 of 23

ADoCSI: Problems seeking solutions

1. How can the location function be implemented transparently ?

3. How can dependent entities retrieve and validate CSI transparently ?

5. How is a certificate path validated ?

7. What is the way this mechanism interacts with dependent entities ?

ADoCSI: Problems seeking solutions (2)

1. How are Agents protected from unauthorised modification or replacement ?

3. How can CSI carried by Agents be protected ?

5. How can an Agent tell a fraudulent Agent Meeting Place ?

7. How can AMPs be protected from DoS attacks ?

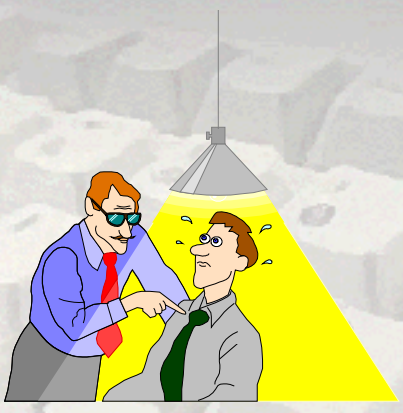
ADoCSI: Problems seeking solutions (8)

1. How can dependent entities be protected against User-CSI Agent replay attacks?

3. How are the Agent Meeting Places protected from malicious Agents ?

5. How can an Agent retrieve CSI for a dependent entity, without letting the AMP know which certificate did it retrieve CSI for ?

Q&A



[Adams98] Adams C., Zuccherato R., A General, Flexible Approach to Certificate Revocation, Entrust Technologies

[EuDir99] Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, 13 December 1999.

[Fox98] Fox B., LaMacchia B., Certificate Revocation: Mechanics and Meaning, In Proceedings of Financial Cryptography 98, LNCS 1465, New York, Springer Verlag

[Gritz97] Gritzalis, S., Spinellis, D. Addressing Threats and Security Issues in World Wide Web Technology, In Proceedings of the 3rd IFIP International Conference on Communications and Multimedia Security, Chapman & Hall, 1997

[Gritz98] Gritzalis S., Iliadis J., Addressing security issues in programming languages for mobile code, In Proceedings of the DEXA '98 9th Workshop of Database and Expert Systems Applications, IEEE Computer Society Press, August 1998

[Hall98] Hallam-Baker P., Ford W., Enhanced CRL Distribution Options, IETF PKIX Working Group, Internet Draft, 7 August 1998, available at http://www.ietf.org/internet drafts/draft-ietf-pkix-ocdp-01.txt

[Hous99] Housley R., Ford W., Polk W., Solo D., Internet X.509 Public Key Infrastructure Certificate and CRL Profile, , IETF Network Working Group, Request for Comments 2459 (Category: Standards Track), January 1999, available at http://www.ietf.org/rfc/rfc2459.txt

[Iliad02] J. Iliadis, S. Gritzalis, D. Gritzalis, "ADoCSI: Towards an Alternative Mechanism for Disseminating Certificate Status Information", to appear

[Iliad00a] J. Iliadis, D. Spinellis, S. Katsikas, D. Gritzalis, B. Preneel. "Evaluating Certificate Status Information Mechanisms". In Proceedinds of the 7th ACM Conference on Computer and Communication Security: CCS '2000, pages 1-8. ACM Press, November 2000.3.

[Iliad00b] Ioannis S. Iliadis, Diomidis Spinellis, Sokratis Katsikas and Bart Preneel, "A Taxonomy of Certificate Status Information Mechanisms", In Information Security Solutions Europe ISSE 2000, Barcelona, Spain, September 2000. European Forum for Electronic Business.

[ISO9594] ISO/IEC 9594-8 (1994), Open Systems Interconnection - The Directory: Authentication Framework.

[Micali96] Micali S., Efficient Certificate Revocation, Technical Memo 542b, Laboratory for Computer Science, Massachusetts Institute of Technology, March 1996

[Myer99] Myers M., Ankney R., Malpani A., Galperin S., Adams C., X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, IETF Network Working Group, Request for Comments 2560 (Category: Standards Track), January 1999, available at http://www.ietf.org/rfc/rfc2560.txt

[Naor98] Naor M., Nissim K., Certificate Revocation and Certificate Update, In Proceedings 7th USENIX Security Symposium, Jan 1998, San Antonio, Texas

[Rivest98] Rivest R., Can We Eliminate Revocation Lists?, In Proceedings of Financial Cryptography 1998, available at http://theory.lcs.mit.edu/~rivest/revocation.ps

[Stub95] Stubblebine S. G., Recent-Secure Authentication: Enforcing Revocation in Distributed Systems, In Proceedings IEEE Symposium on Research in Security and Privacy, pages 224-234, May 1995, Oakland

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997