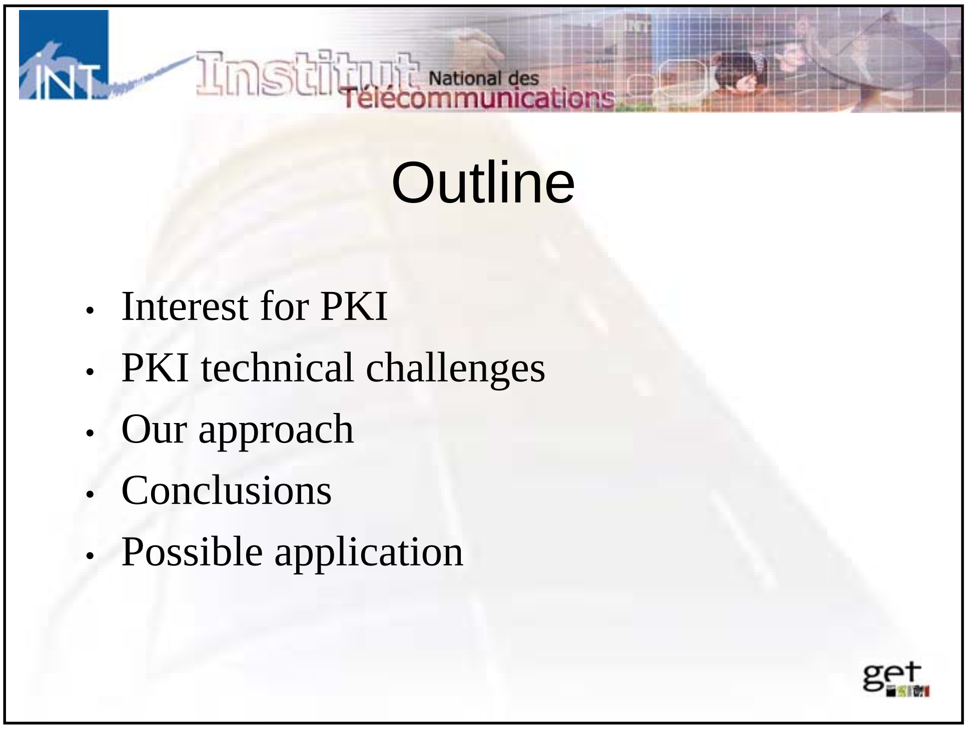
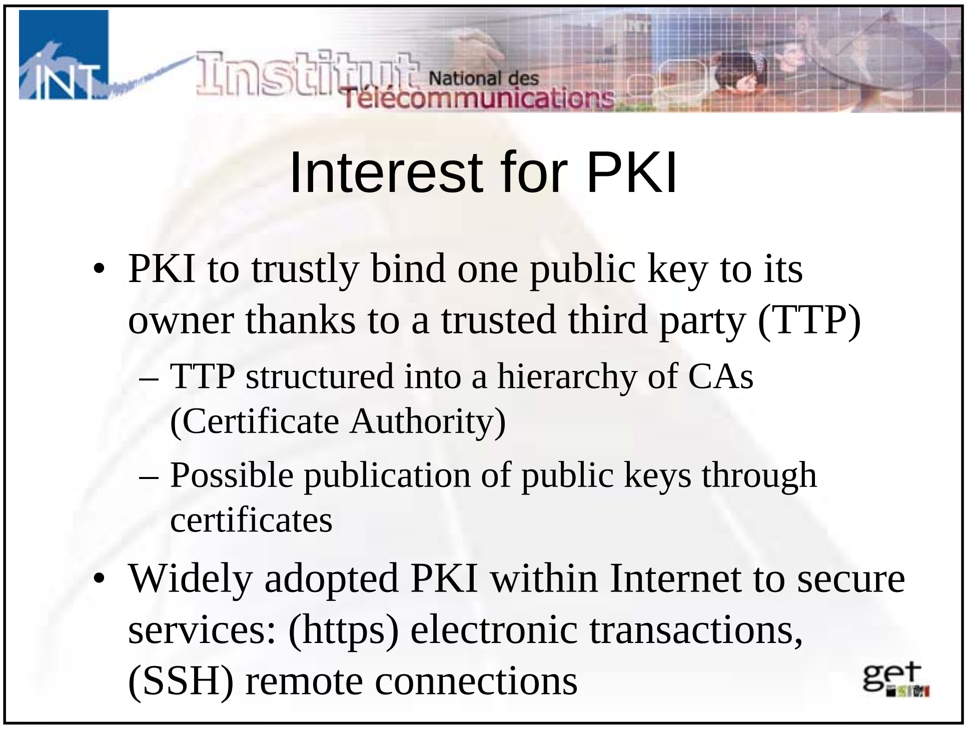
A PKI approach targeting the provision of a minimum security level within Internet

Maryline Laurent-Maknavicius
GET/INT - CNRS/SAMOVAR



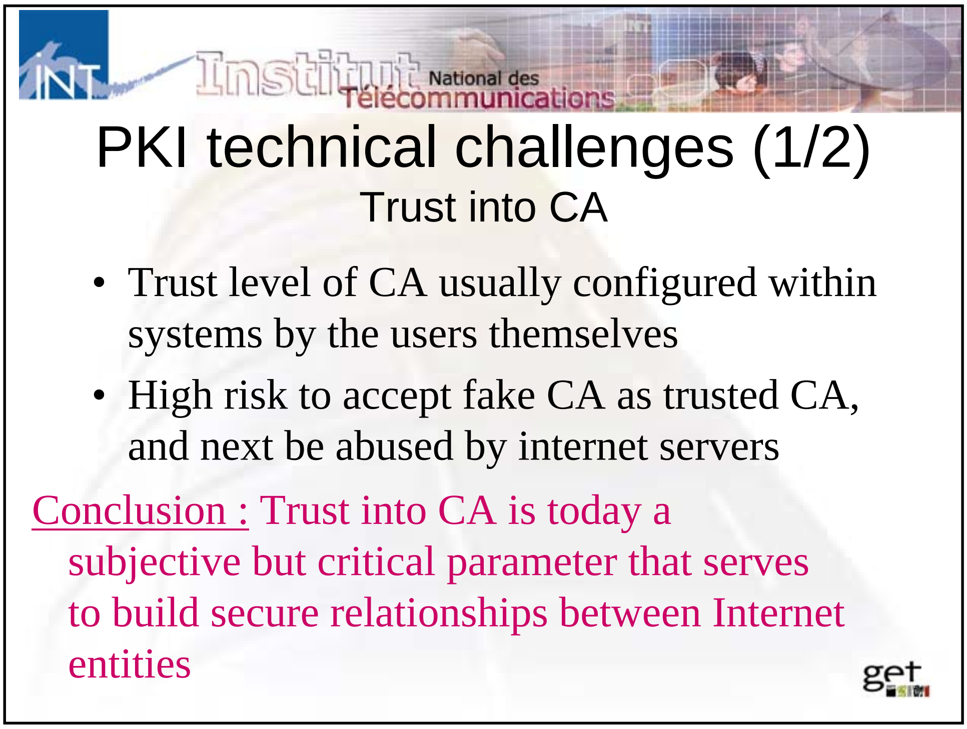
Outline

- Interest for PKI
- PKI technical challenges
- Our approach
- Conclusions
- Possible application



Interest for PKI

- PKI to trustly bind one public key to its owner thanks to a trusted third party (TTP)
  - TTP structured into a hierarchy of CAs (Certificate Authority)
  - Possible publication of public keys through certificates
- Widely adopted PKI within Internet to secure services: (https) electronic transactions, (SSH) remote connections

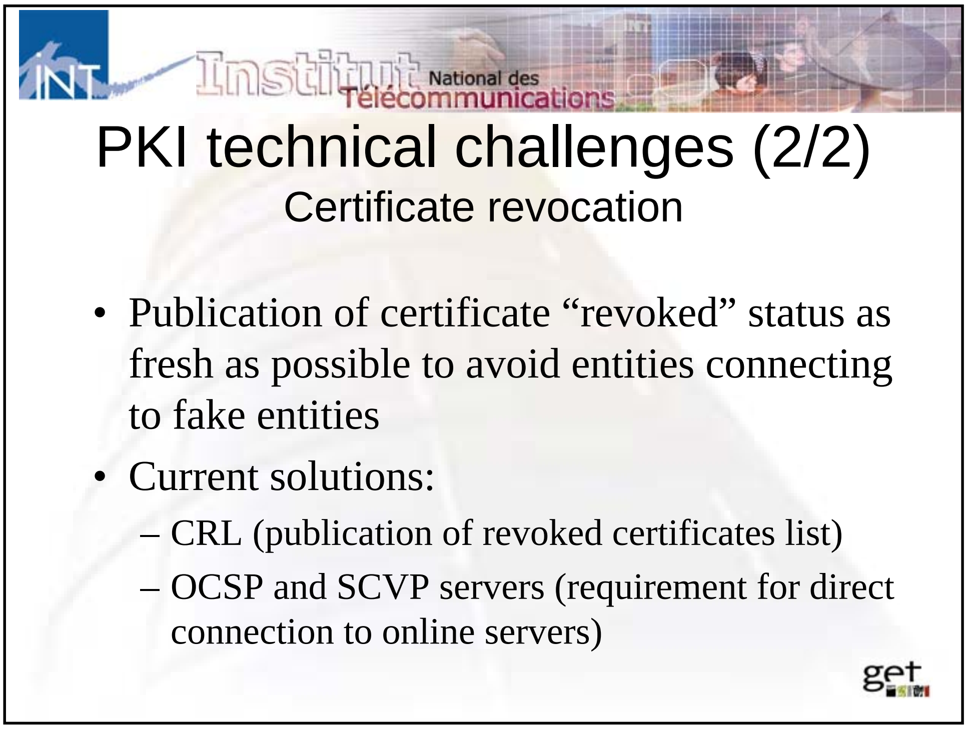


PKI technical challenges (1/2)

Trust into CA

- Trust level of CA usually configured within systems by the users themselves
- High risk to accept fake CA as trusted CA, and next be abused by internet servers

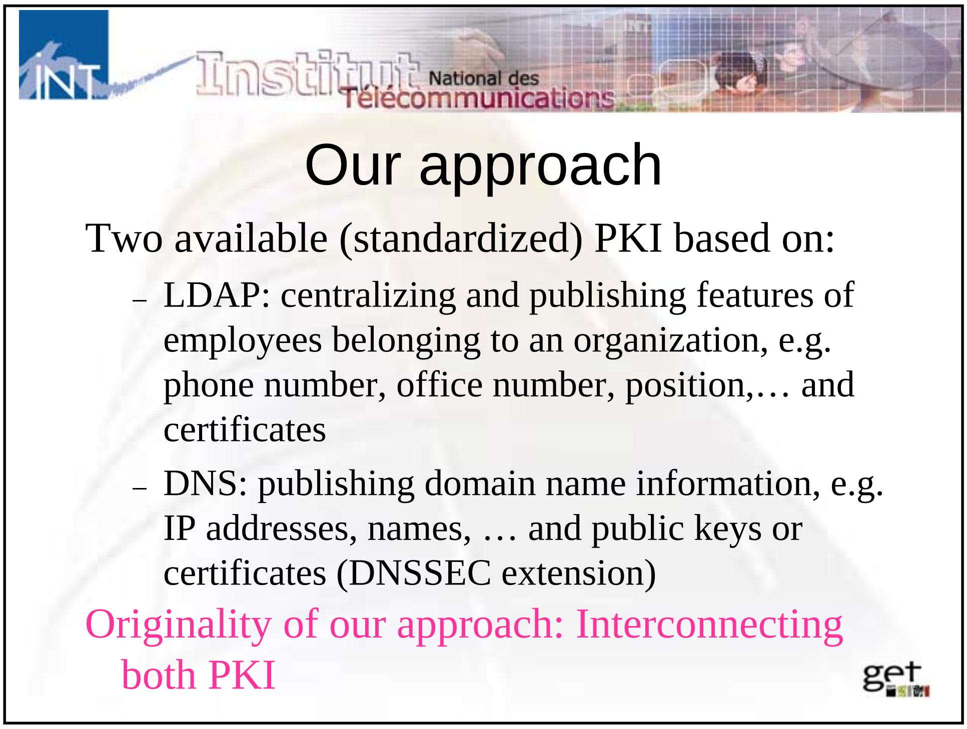
Conclusion : Trust into CA is today a subjective but critical parameter that serves to build secure relationships between Internet entities



PKI technical challenges (2/2)

Certificate revocation

- Publication of certificate “revoked” status as fresh as possible to avoid entities connecting to fake entities
- Current solutions:
  - CRL (publication of revoked certificates list)
  - OCSP and SCVP servers (requirement for direct connection to online servers)

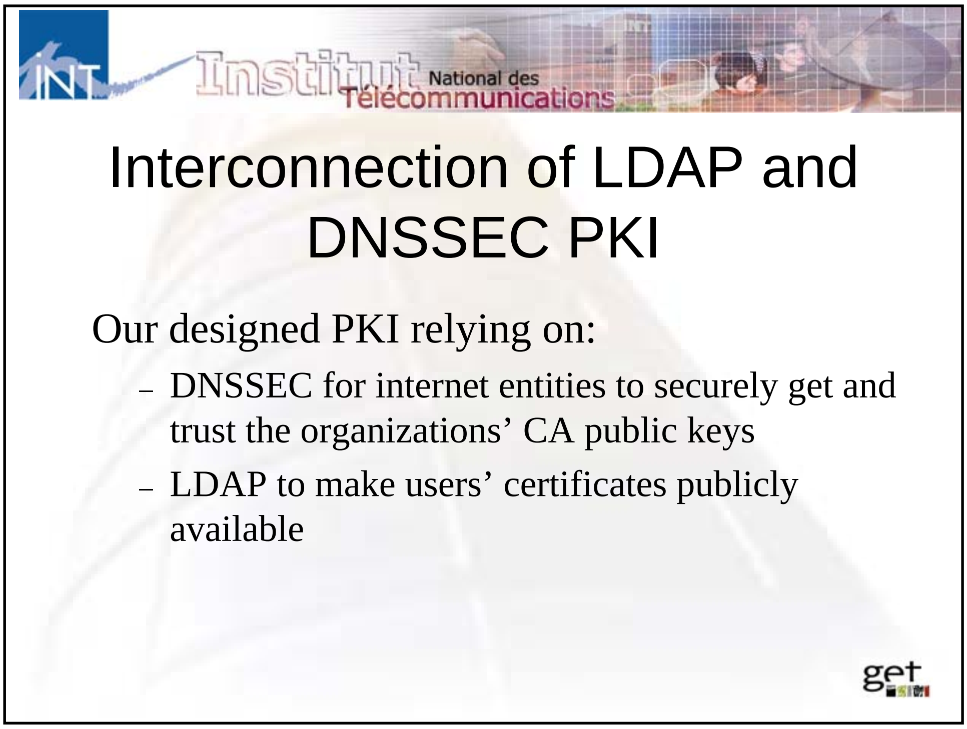


Our approach

Two available (standardized) PKI based on:

- LDAP: centralizing and publishing features of employees belonging to an organization, e.g. phone number, office number, position,… and certificates
- DNS: publishing domain name information, e.g. IP addresses, names, … and public keys or certificates (DNSSEC extension)

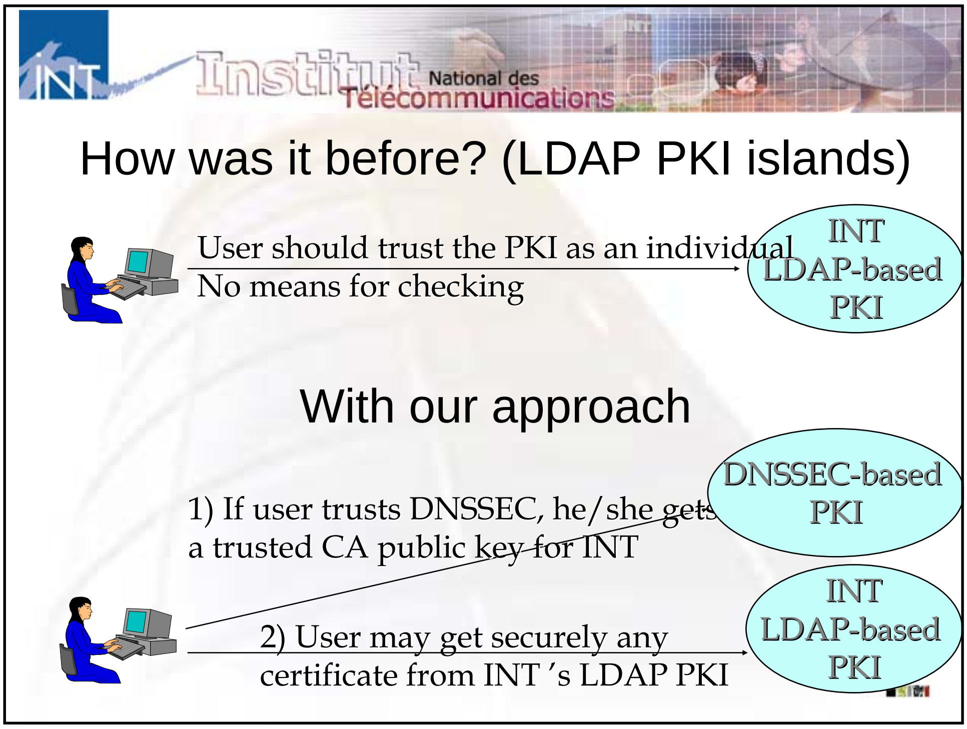
Originality of our approach: Interconnecting both PKI



Interconnection of LDAP and DNSSEC PKI

Our designed PKI relying on:

- DNSSEC for internet entities to securely get and trust the organizations' CA public keys
- LDAP to make users' certificates publicly available



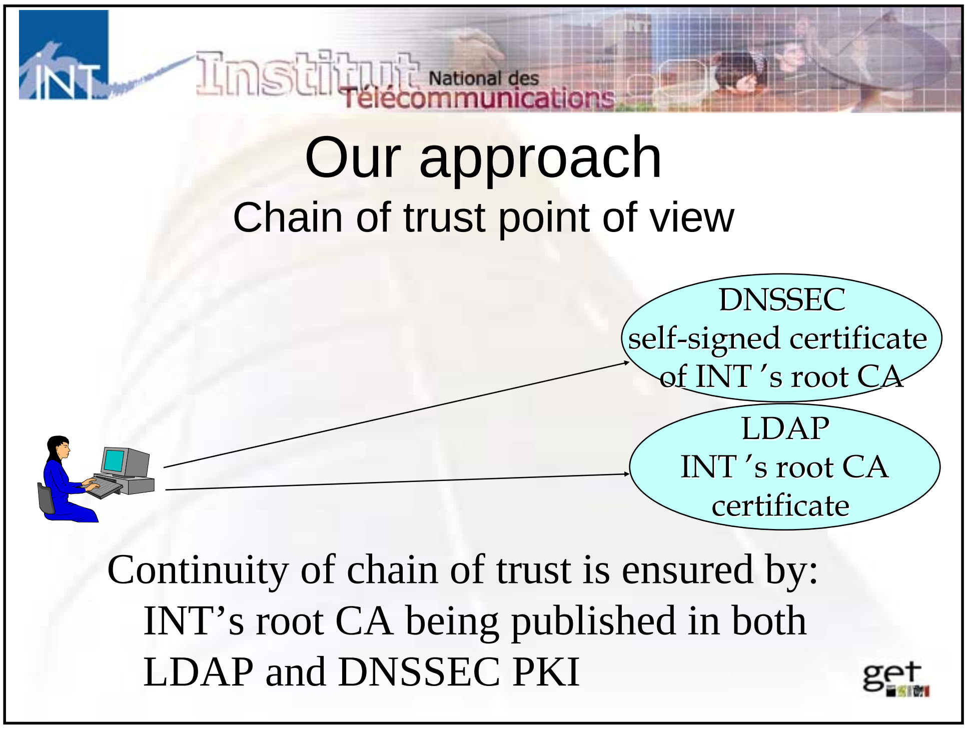
How was it before? (LDAP PKI islands)

User should trust the PKI as an individual
No means for checking

With our approach

1) If user trusts DNSSEC, he/she gets a trusted CA public key for INT

2) User may get securely any certificate from INT 's LDAP PKI



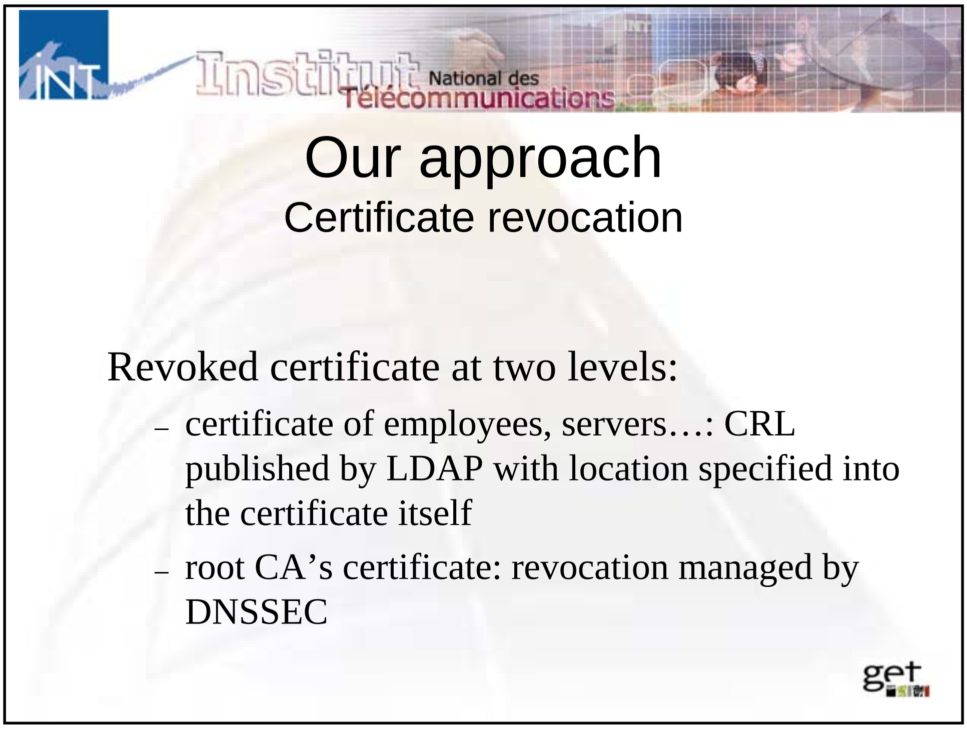
Our approach

Chain of trust point of view

DNSSEC
self-signed certificate
of INT ′s root CA

LDAP
INT ′s root CA
certificate

Continuity of chain of trust is ensured by:
INT’s root CA being published in both LDAP and DNSSEC PKI

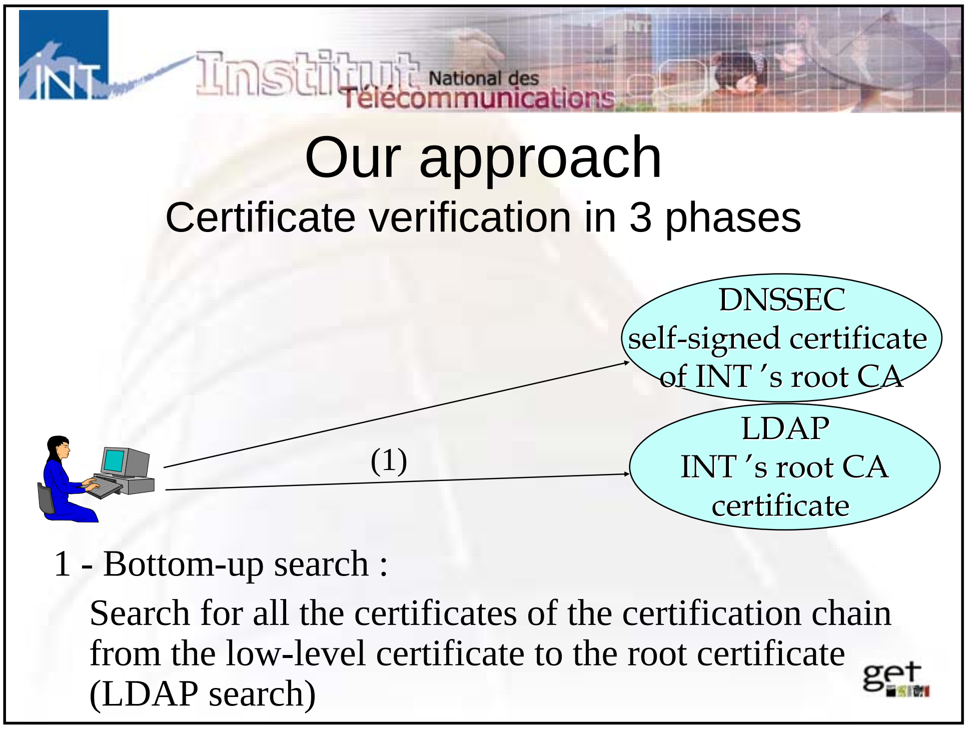


Our approach

Certificate revocation

Revoked certificate at two levels:

- certificate of employees, servers…: CRL published by LDAP with location specified into the certificate itself
- root CA’s certificate: revocation managed by DNSSEC



Our approach

Certificate verification in 3 phases

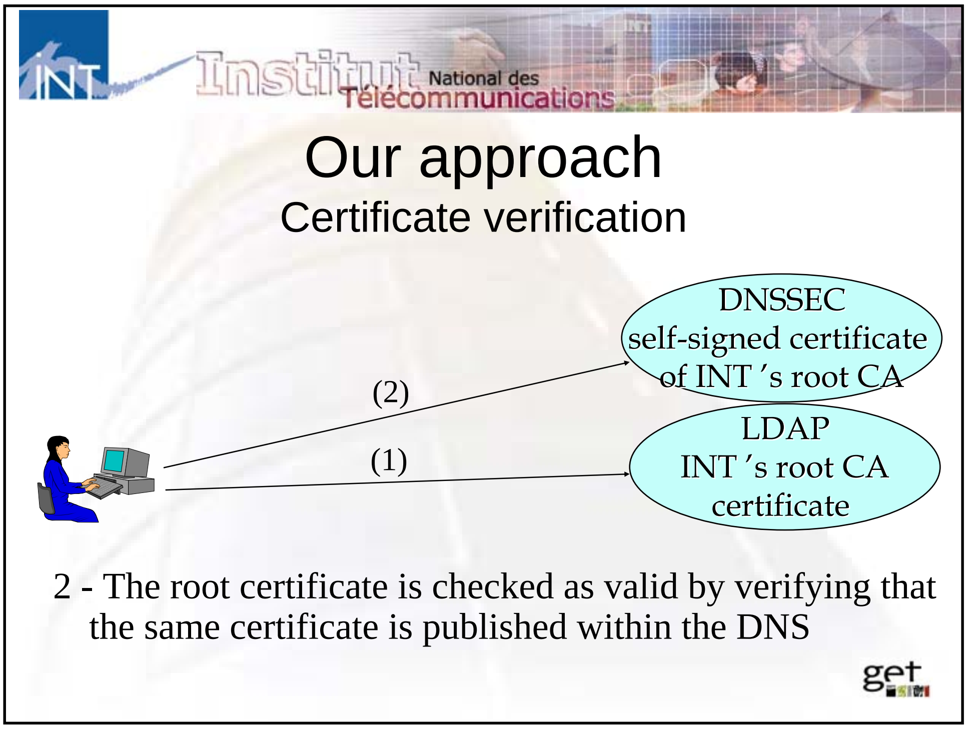
DNSSEC
self-signed certificate
of INT's root CA

LDAP
INT's root CA
certificate

(1)

1 - Bottom-up search :

Search for all the certificates of the certification chain from the low-level certificate to the root certificate (LDAP search)



Our approach

Certificate verification

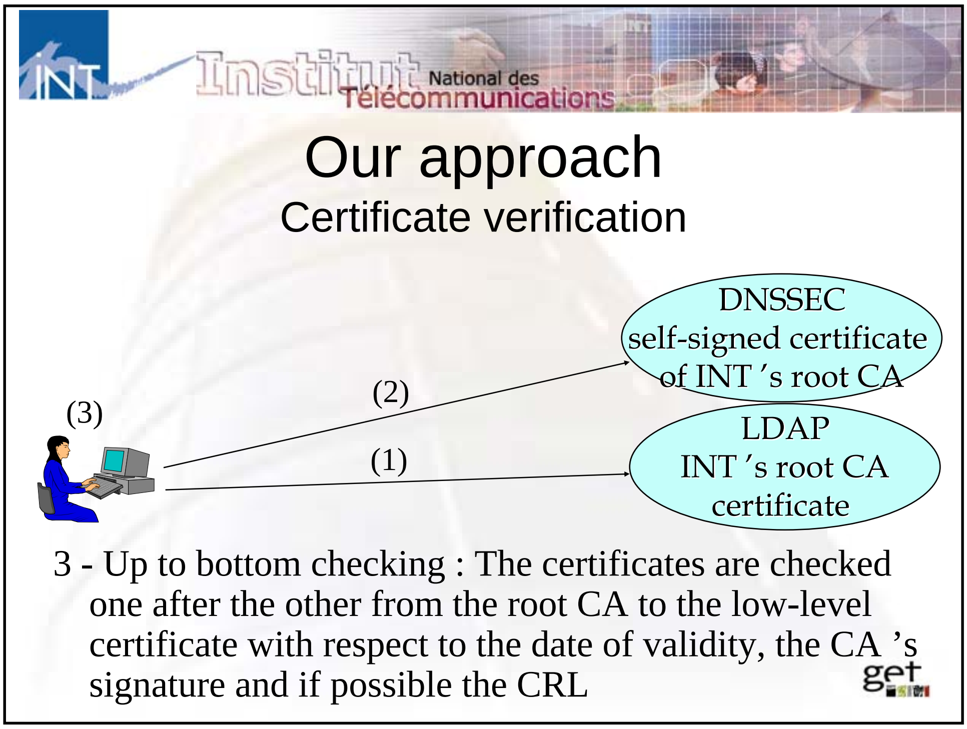
DNSSEC
self-signed certificate
of INT's root CA

LDAP
INT's root CA
certificate

(2)

(1)

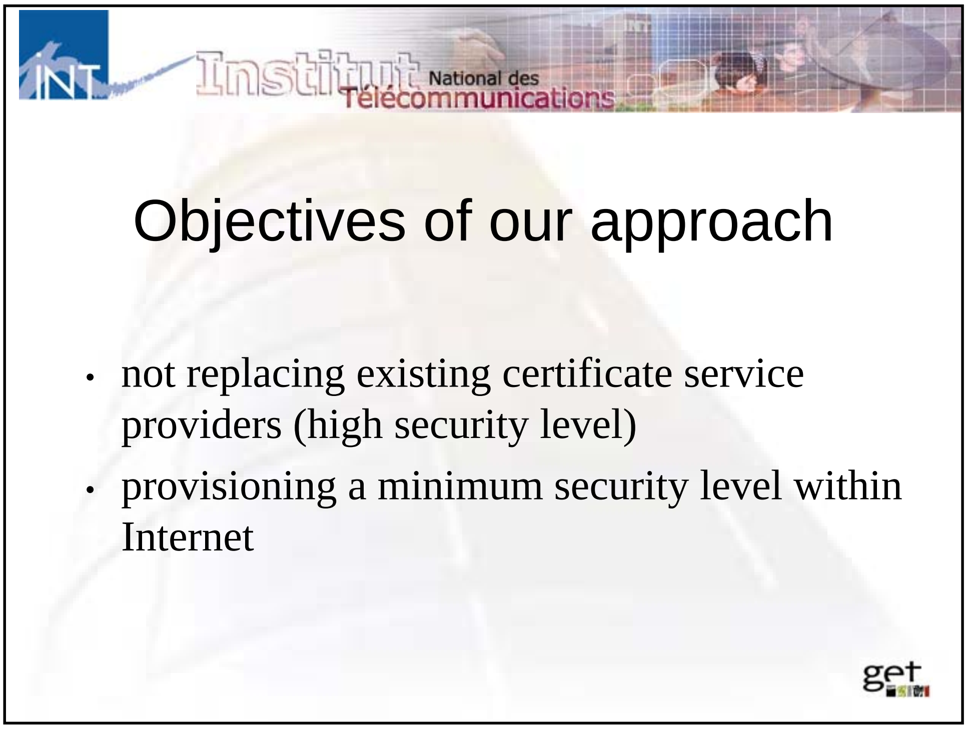
2 - The root certificate is checked as valid by verifying that the same certificate is published within the DNS



Our approach

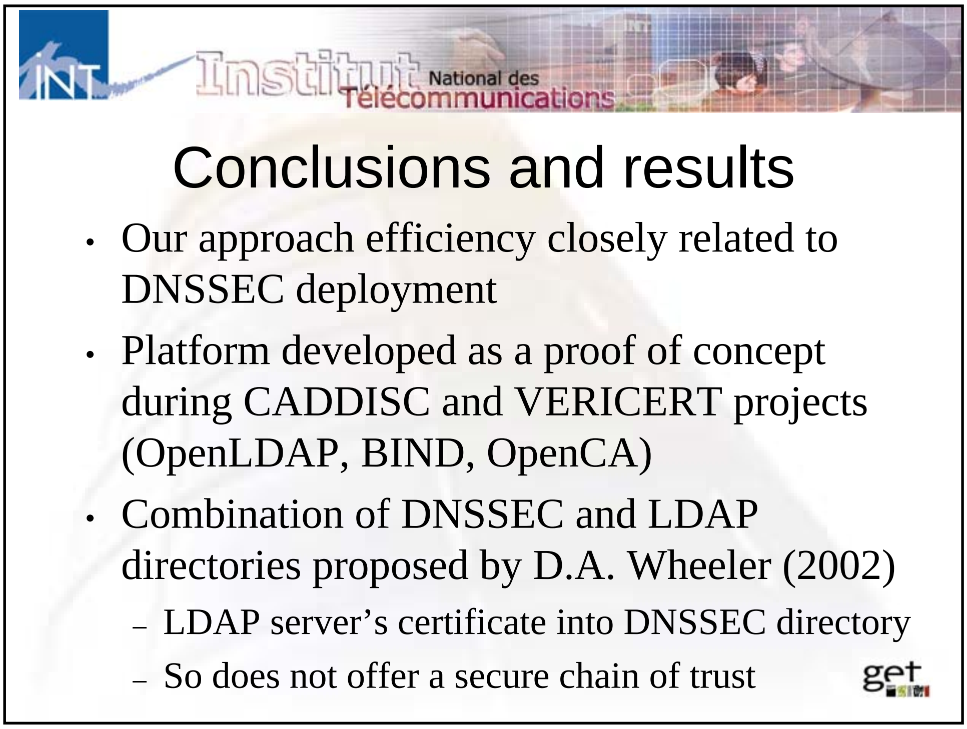
Certificate verification

3 - Up to bottom checking : The certificates are checked one after the other from the root CA to the low-level certificate with respect to the date of validity, the CA ’s signature and if possible the CRL



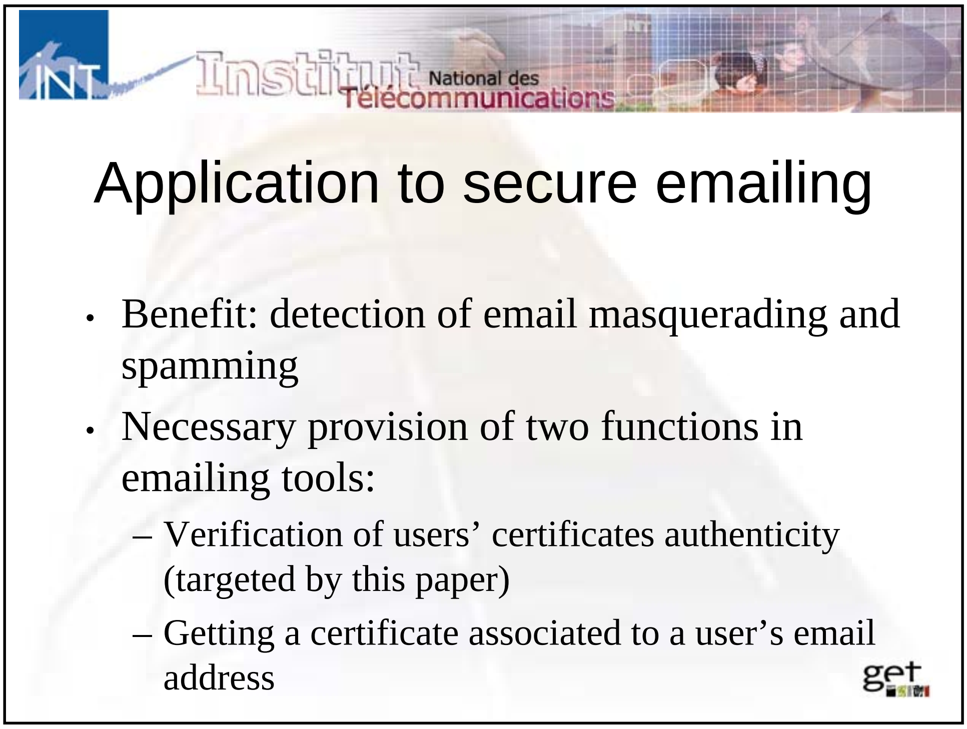
Objectives of our approach

- not replacing existing certificate service providers (high security level)
- provisioning a minimum security level within Internet



Conclusions and results

- Our approach efficiency closely related to DNSSEC deployment
- Platform developed as a proof of concept during CADDISC and VERICERT projects (OpenLDAP, BIND, OpenCA)
- Combination of DNSSEC and LDAP directories proposed by D.A. Wheeler (2002)
  - LDAP server's certificate into DNSSEC directory
  - So does not offer a secure chain of trust



Application to secure emailing

- Benefit: detection of email masquerading and spamming
- Necessary provision of two functions in emailing tools:
  - Verification of users' certificates authenticity (targeted by this paper)
  - Getting a certificate associated to a user's email address