

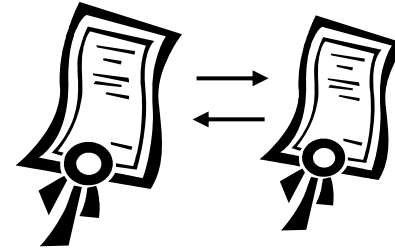


# Cross-Certification: Bridging the Gaps between Disconnected Hierarchies

# Objectives

- Emphasize applicability of cross-certification
- Raise awareness of current PKI solutions at CERT/CC and what services are supported
- Discuss preliminary plans for our next generation PKI
- Open dialog with CSIRTs to consider prospective cross-certification opportunities

# Cross-Certification



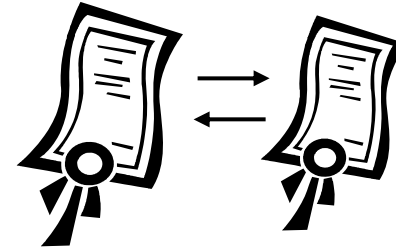
## Applicability:

- CSIRTs with National Responsibility (CNRs)
  - JPCERT/CC
- U.S. Government sector – HSPD-12
- U.S. Military – DoD PKI/CAC Cards

## Other areas where PKI is gaining ground:

- Large industry support
- Major deployment in Europe (GRID)
- Higher Education – Australia, Canada, U.S.

# Cross-Certification



## PKI Offers:

- 2-factor authentication for technological collaboration and resource sharing
- Inter-institution trust models for identity management, authentication and encryption
- Absolute control over accessibility of information
- Economy of scale, ease of use, and interoperability
- Growing support based on wide deployment across many areas of the community

# CERT/CC Knowledgebase Summary

- Four web-based components

- Special Communications

- Vulnerability Cards

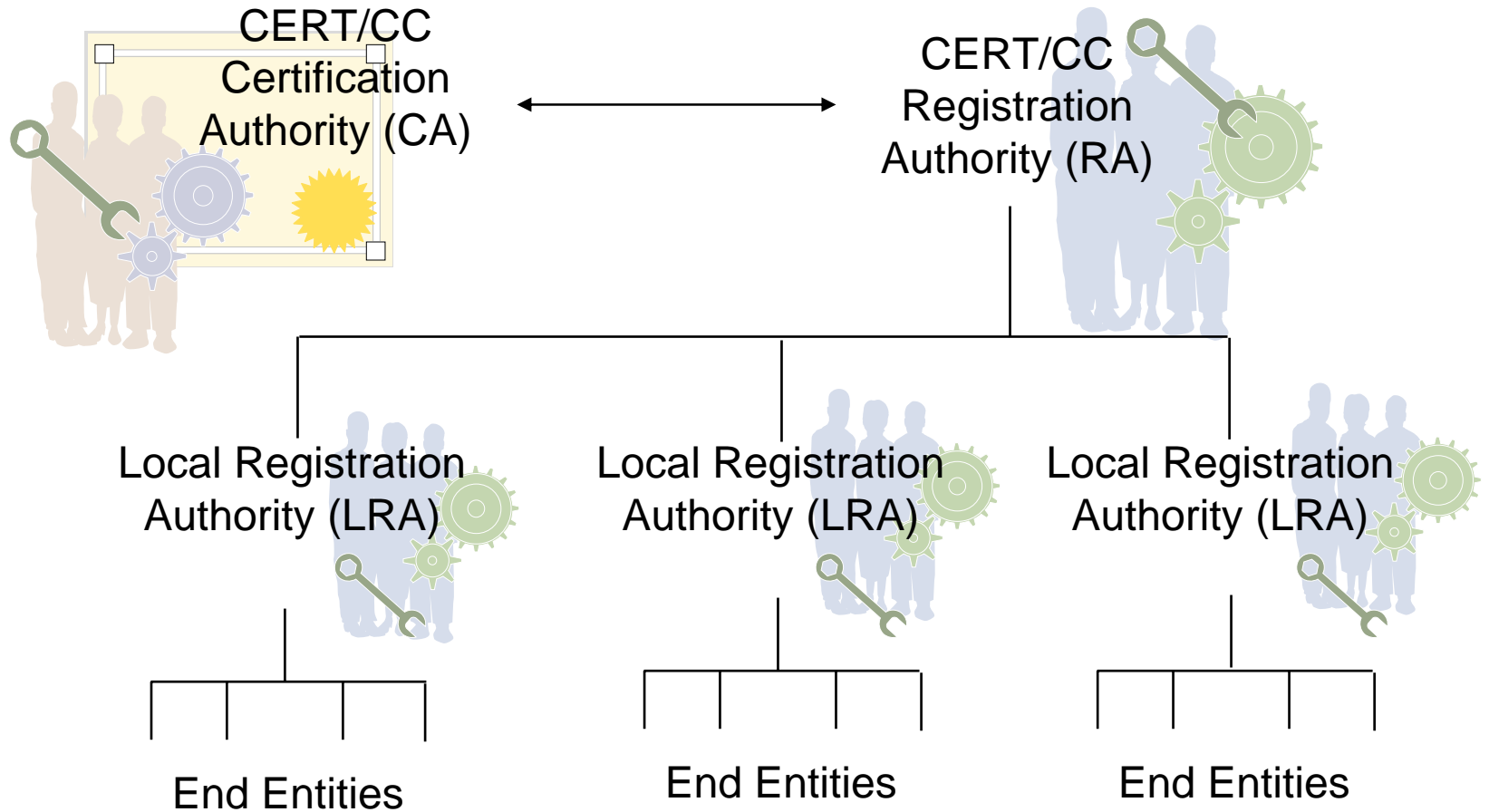
**Restricted – x.509  
certificate access**

- Vulnerability Notes

- Technical Alerts

**Public**

# Components of the CERT/CC PKI



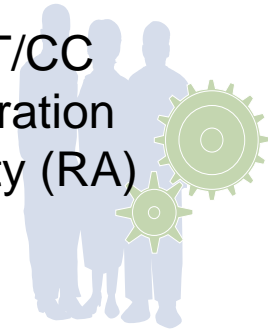
# Local Registration Authority

- Individual(s) trained to use the RA to manage registration requests within their ORG
- Typically security managers, team leads, or ISOs
- Support for Primary and Alternate
- One ORG can have many LRAs



# Registration Authority

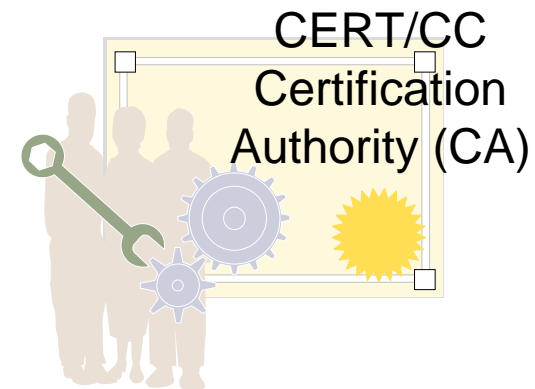
CERT/CC  
Registration  
Authority (RA)



- Web interface comprising
  - Webform for initiating registration requests
  - Administrative Console for managing requests
- 3-step registration process
- Organization Identification Number (OIN)
- Identity authentication performed by the LRA

# Certification Authority

- KBCA issues end-entity certificates (EEC's) for
  - U.S. Government
  - U.S. Military
  - CERT/CC staff
  - Approved CSIRTs with national responsibility (under NDA)
  - Approved security researchers (under NDA)



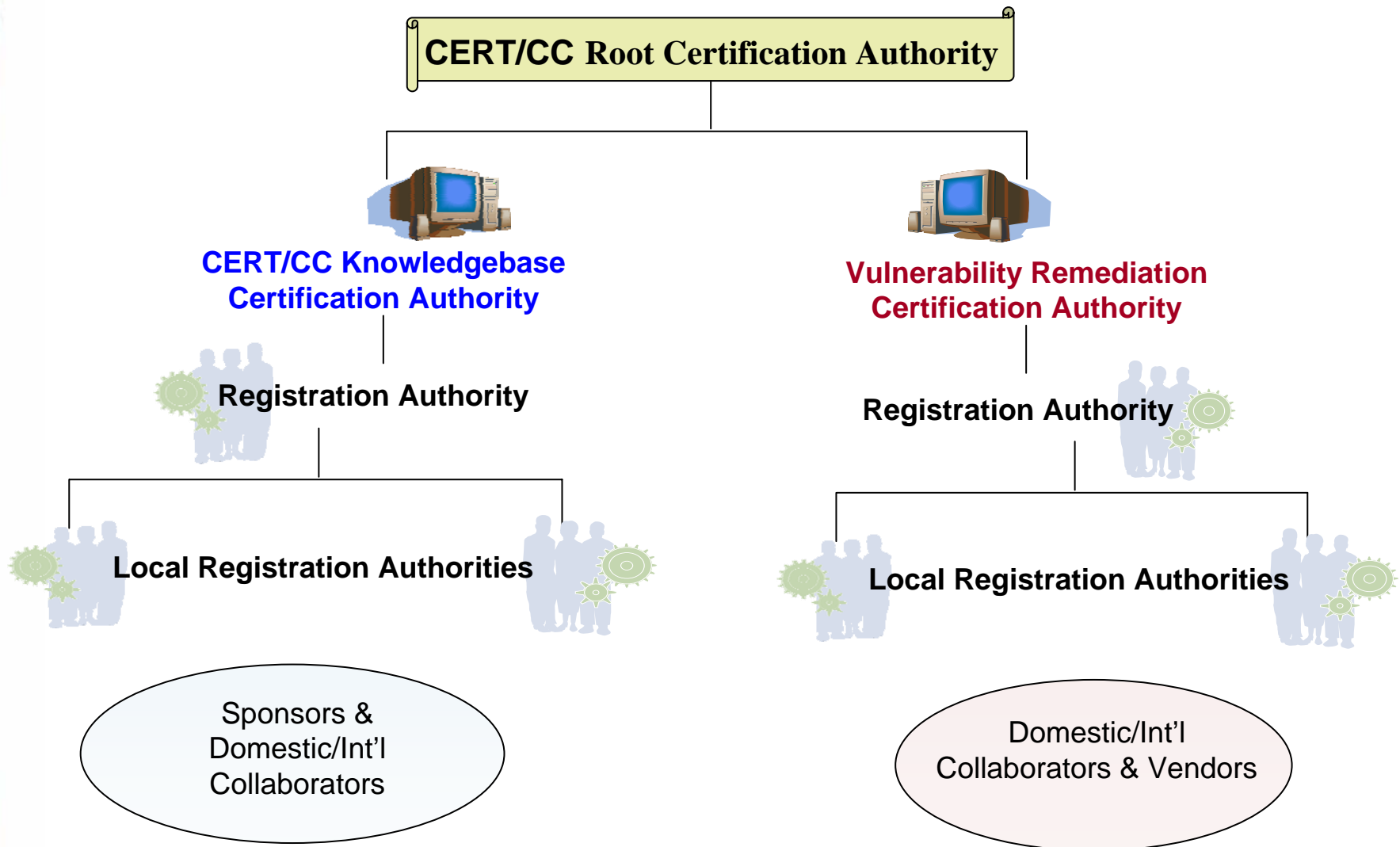
# Certification Authority

- Current CA certificate generated in Sep-2003
- 5-year validity period - expires in Sep-2008

# Next Generation PKI

- Beginning stages of project planning
- Strategy focused on broadening scope of services
  - Restricted components of CERT/CC Knowledgebase
  - Vendor portal for information exchange
  - Vendor brokering service to improve vulnerability coordination processes
  - Cross-certification with other CNRs working in this area toward global effort of vulnerability research/remediation

# PKI Model – External CAs



# Policy Governance



- Four levels of assurance
  - High
  - Medium
  - Basic
  - Rudimentary

# Next Steps

- Draft project plan that maps to business requirements
- PKI project planning
  - PKI Project Proposal
  - Certificate Policy/Certification Practices Statement
  - Select a list of applications
  - Evaluate applications against business requirements
  - Begin decommissioning of current CA (with contingency plan)
- Get the word out

# Questions?

# CERT® Contact Information

CERT Coordination Center  
Software Engineering Institute  
Carnegie Mellon University  
4500 Fifth Avenue  
Pittsburgh PA 15213  
USA

Hotline: +1 412 268 7090 CERT personnel answer 8:00 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412 268 6989

Web: <http://www.cert.org/>

Email: [cert@cert.org](mailto:cert@cert.org)