PKI : The role of TTP's for the Development of secure Transaction Systems

EPIC

Introduction

- Electronic transactions : how safe are they? Common security threats
- Security schemes and solutions used before the development of PKI
- The role of PKI in securing transactions. Providing secure transactions in insecure networks

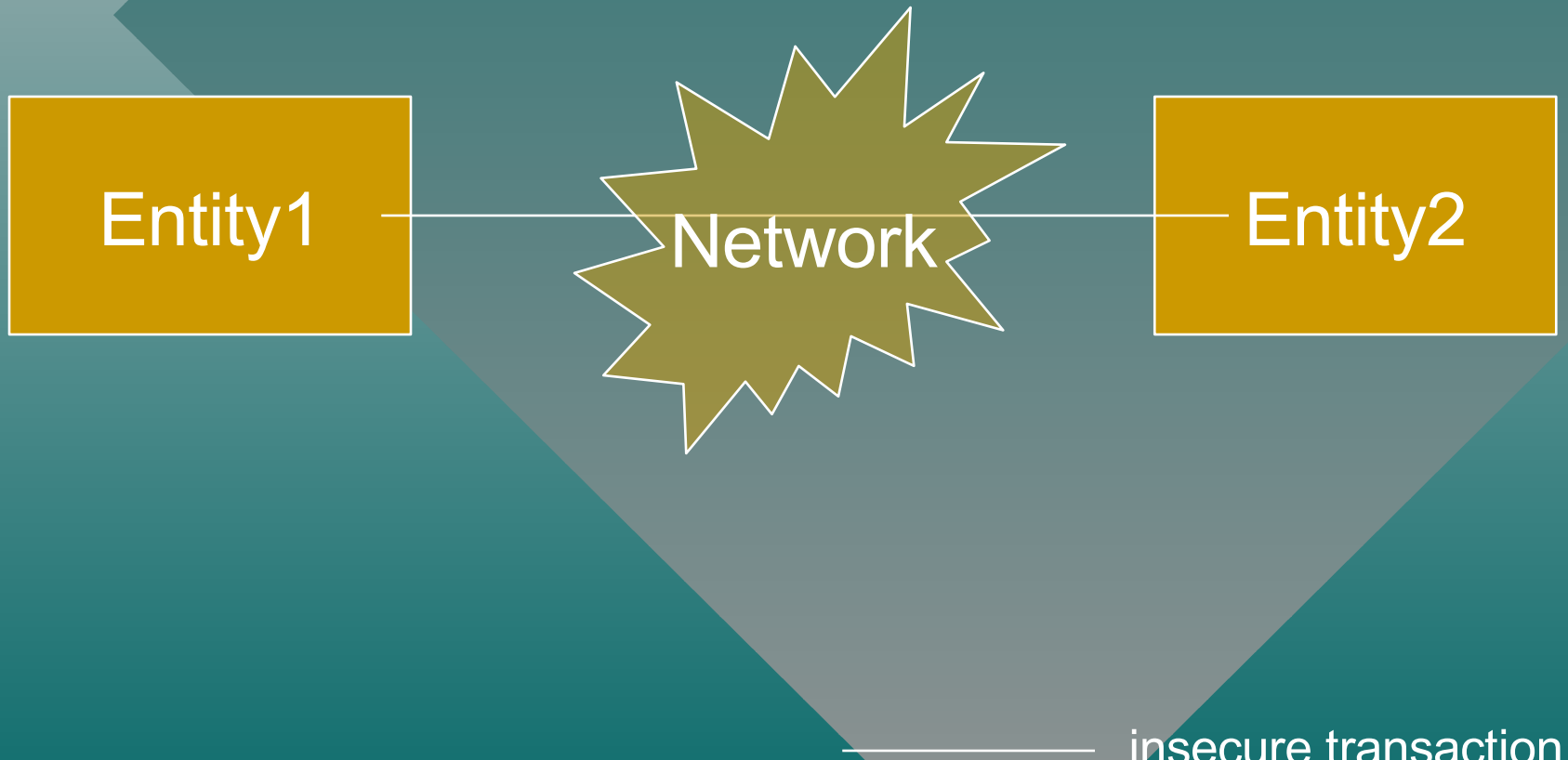
Overview

- Identification of security threats in electronic transactions
- Confrontation with security threats through PKI provisions
- TTP : the cornerstone of a Public Key Infrastructure. A general overview
- TTP services and functions

Security threats in electronic transactions

- monitoring of communication lines
- Non-authorised modification of (in-transit) information
- Masquerade - Web spoofing
- Password stealing
- Unauthorised access
- Key personnel and physical insecurity

Insecure electronic transactions



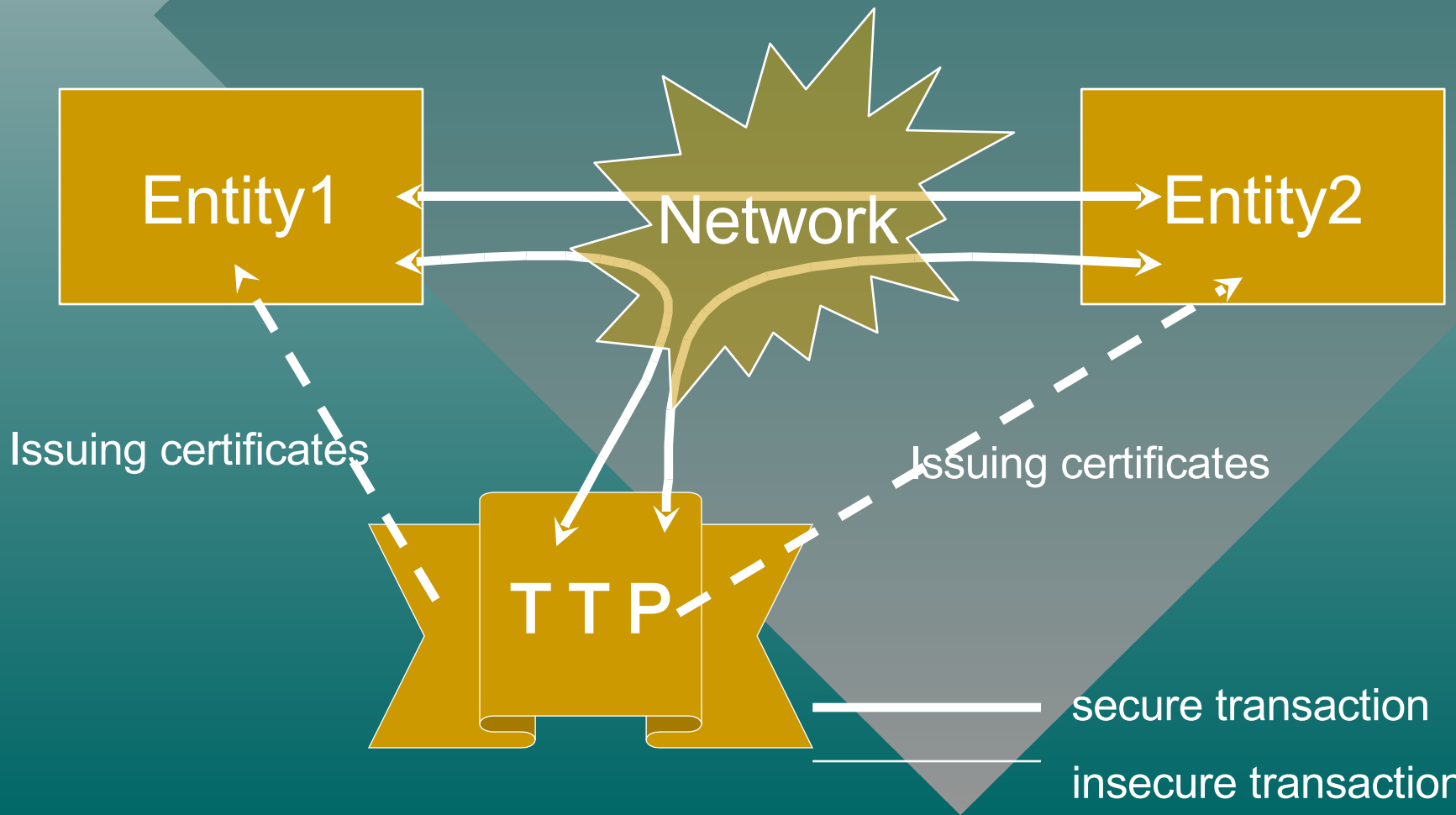
Confrontation with security threats through PKI provisions

- *monitoring of communication lines*
  Encryption with randomly generated shared session key
- *shared session key stealing/guessing*
  -cryptographically secure random key generators
  -encryption of shared session key with the public key of the receiving entity
- *Non-authorised modification of (in-transit) information*
  secure hashing algorithms for message authentication codes

Confrontation with security threats through PKI provisions

- *Masquerade - Web spoofing*
  Exchange of X509v3 certificates and verification against a Directory
- *Password stealing*
  Passwords are never transmitted in the network
- *Unauthorised access*
  Local ACL. Authentication by certificate verification

TTP : Securing electronic transactions



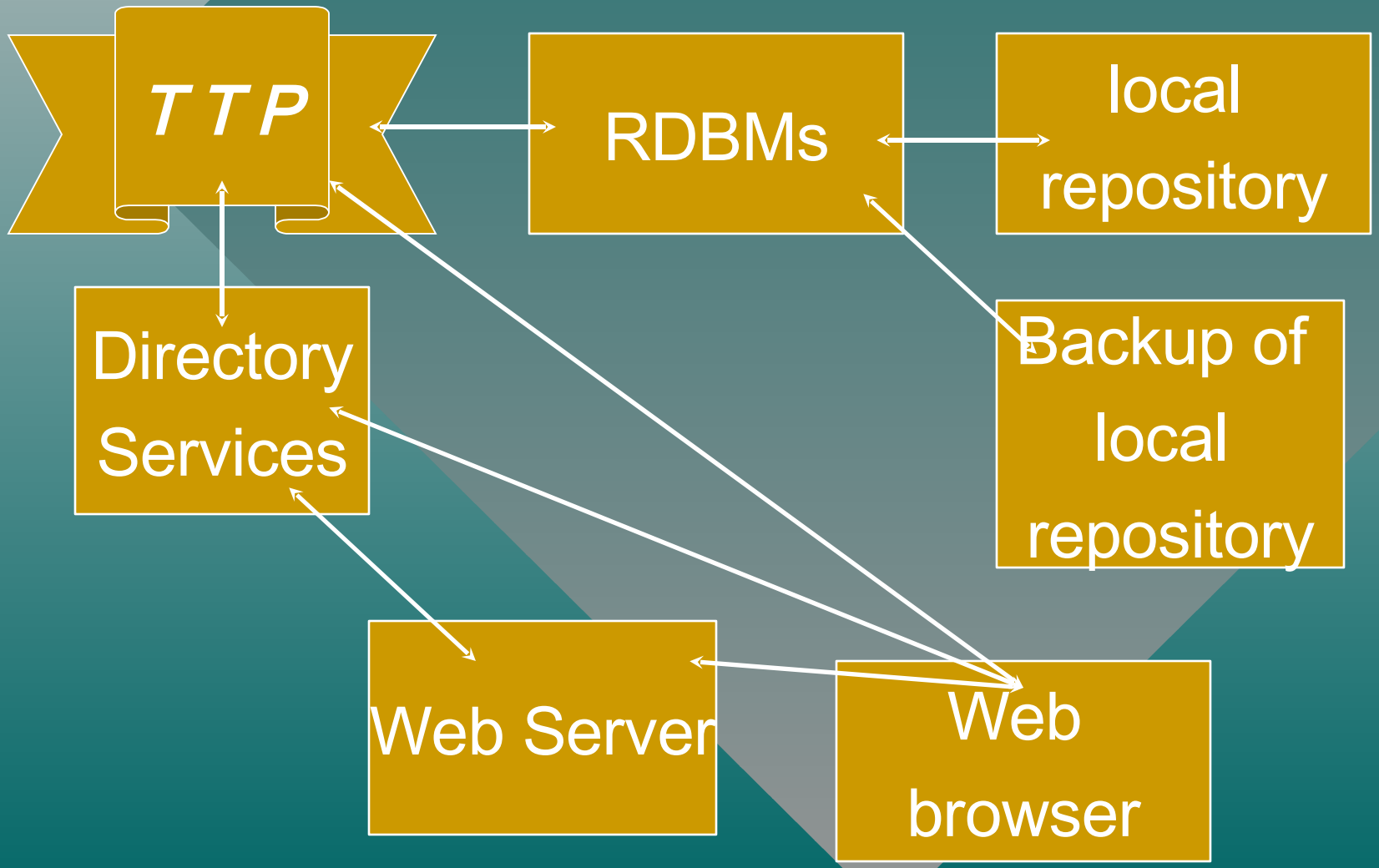
TTP : the cornerstone of a Public Key Infrastructure. A general overview

TTP : "an impartial organisation delivering business confidence, through commercial and technical security features, to an electronic transaction"

TTP : the cornerstone of a Public Key Infrastructure. Technical Infrastructure

- *Directory Services* acting as repositories of identification and authentication information of the entities participating in the security scheme.
- *Certificate Servers* providing the X.509v3 certificates and thus validating the signatures of the abovementioned entities
- *Content Servers* operating as platforms for the dissemination of data and the remote execution of application. If the network that is used is the Internet, then the content servers are Web Servers.
- *Network client* which provides the capability of accessing the information stored in the content servers, executing remote applications and accept and store certificates for use by the entity. If the network used is the Internet, then the network client is a Web browser

TTP : the cornerstone of a Public Key Infrastructure. Technical Infrastructure



TTP services and functions

- *Electronic Registration*
- *Key Personalisation, Generation, and Repository*
- *Certificates: Structure, Generation, Distribution, Storage, and Retrieval*
- *Certificate Directory Management*
- *CRLs: Structure, Generation and Maintenance, Distribution, Storage, and Retrieval*
- *Auditing*