The Open Systems Interconnection (OSI) Model
Secure Communication in Open Networks
Digital Signature

IAG0650

Spring Semester 2017

Dirk Draheim

TALLINN UNIVERSITY OF TECHNOLOGY

LSS

Large-Scale Systems Group
Tallinn University of Technology

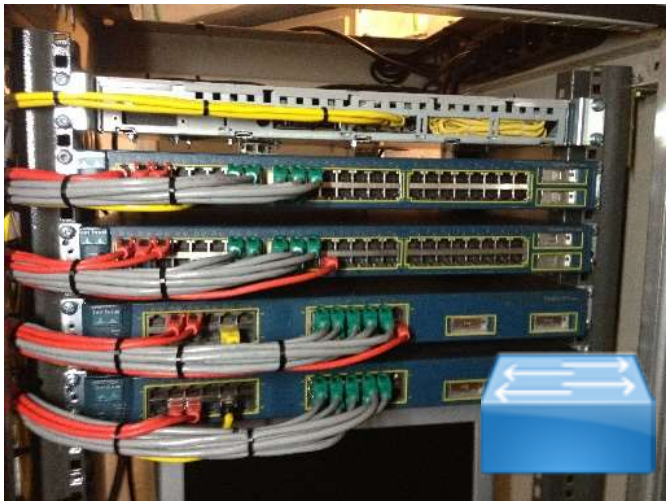
OSI Model / OSI Layer Model
Open Systems Interconnection model

LSS
Large-Scale Systems Group
Tallinn University of Technology

OSI Layer			DoD Layer	Internet Protocols		Devices Components	Objects		
7	Application		Process	**HTTP**, HTTPS, FTP, SMTP, NCP, **SOAP**, DNS, DHCP, RADIUS SSH,**SSL**,**TSL**,...		Gateway Content Switch Proxy	data	application-oriented	end-to-end
6	Presentation								
5	Session								
4	Transport		Host-to-Host	**TCP**, UDP,...		*Firewall*	**segment** datagram	transport-oriented	
3	Network		Internet	**IP** (IPv4, IPv6)...		Router, NAT Layer-3-Switch	packet		point-to-point
2	Data Link	*2a Logical Link*	Net Access	**Ethernet**	PPP	Switch Bridge	frame		
		2b MAC (Medium Access)							
1	Physical				SONET ADSL	Repeater, Hub Network Cable	bit symbol		

Internet Devices

Large-Scale Systems Group
Tallinn University of Technology



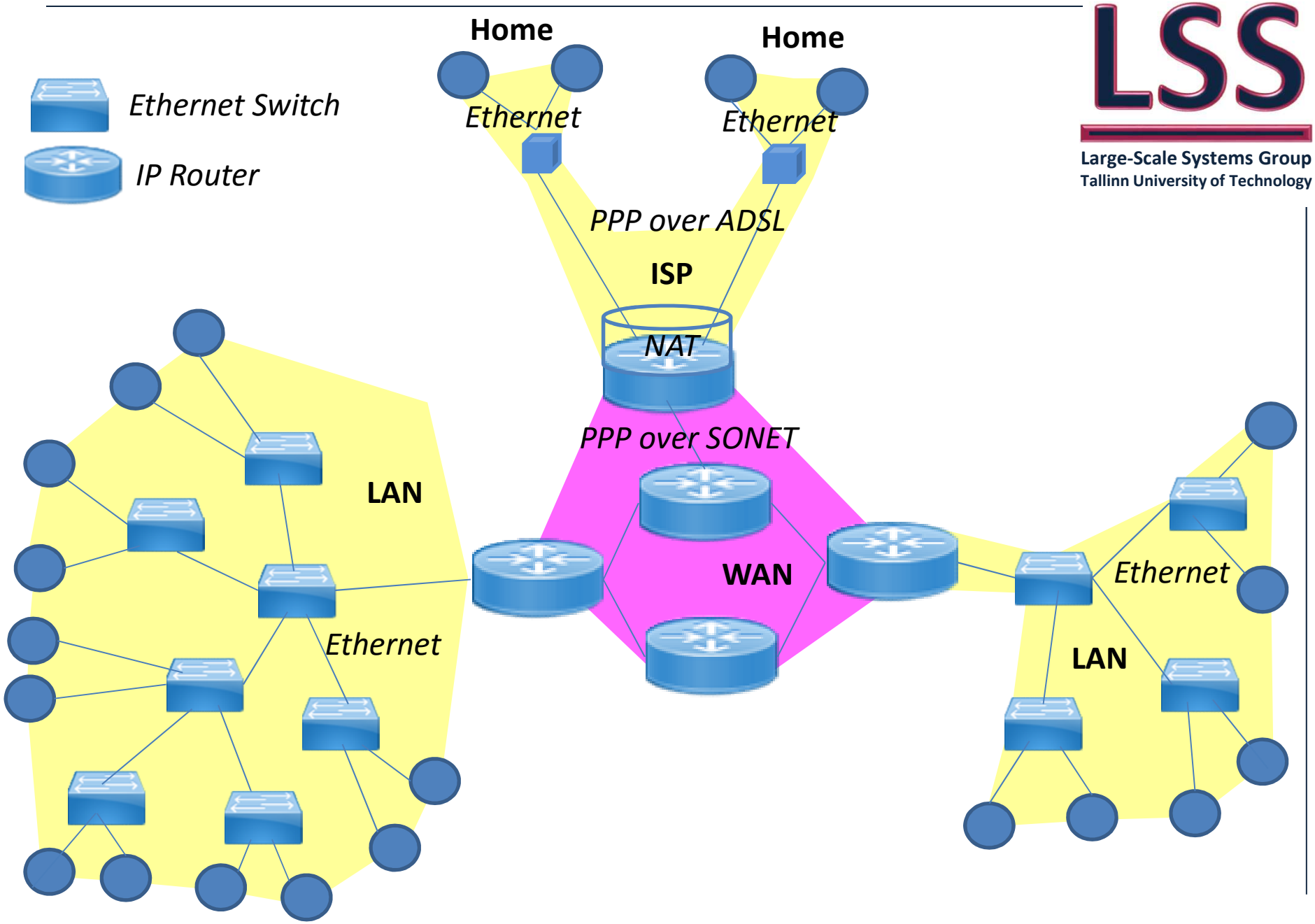
Switch

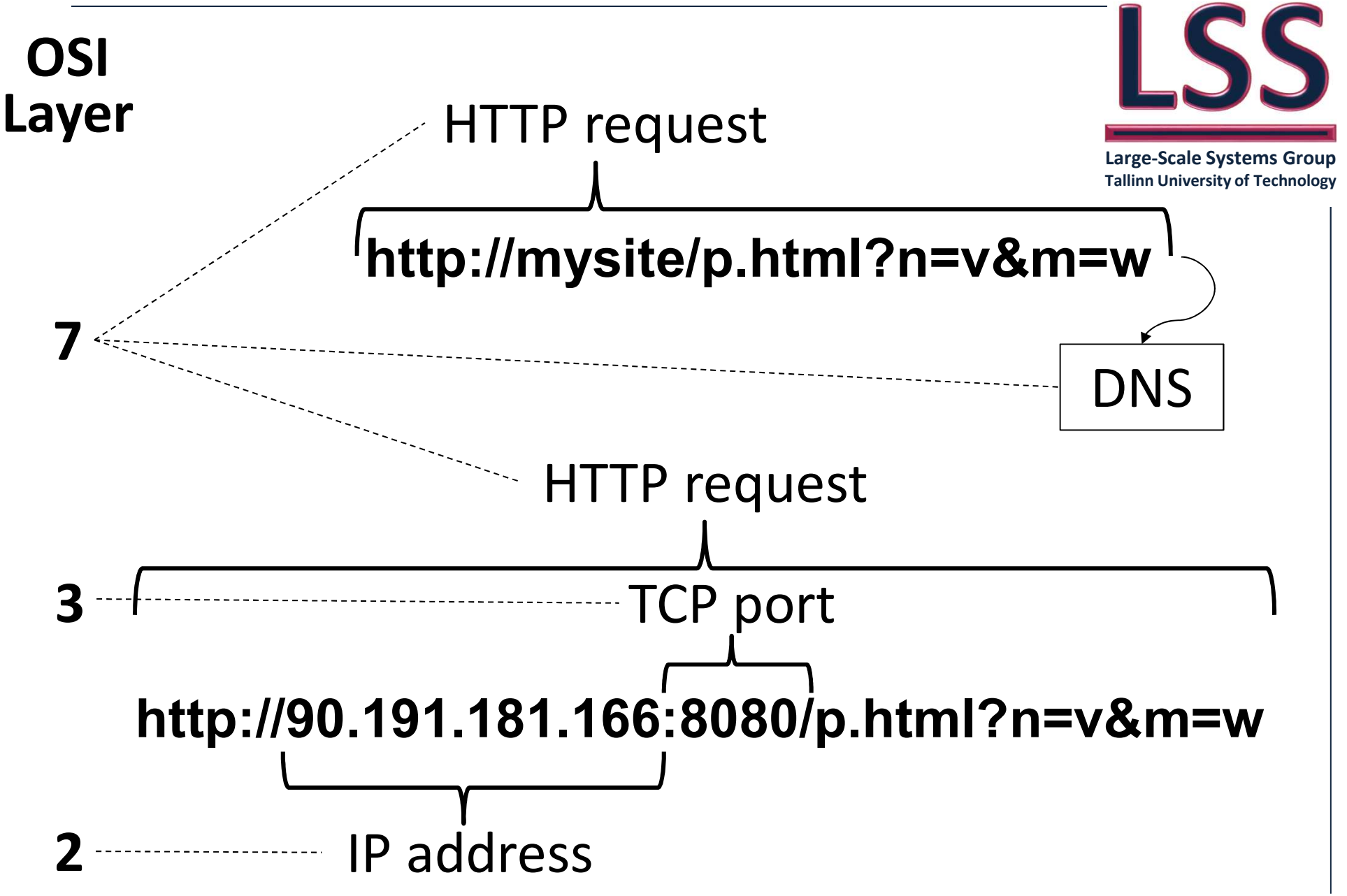
Router

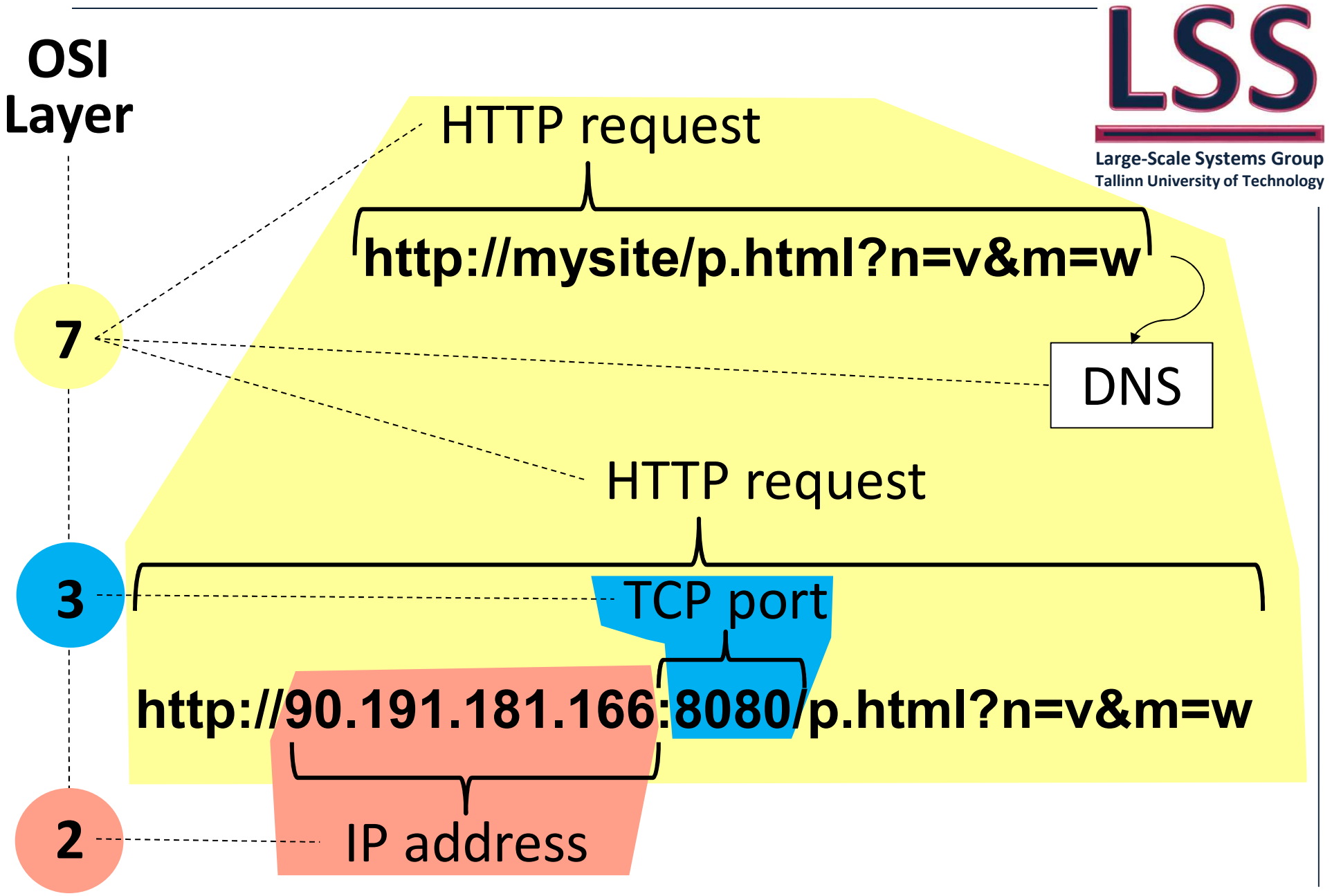
Hub

DSL Gateway

Firewall


Ethernet Switch
IP Router
Home
Home
Ethernet
Ethernet
PPP over ADSL
ISP
NAT
PPP over SONET
LAN
WAN
Ethernet
Ethernet
LAN

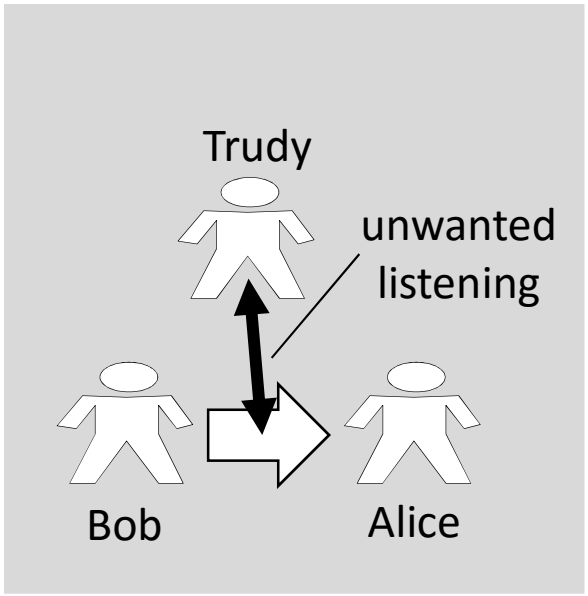

OSI Layer
HTTP request
http://mysite/p.html?n=v&m=w
7
DNS
HTTP request
3
TCP port
http://90.191.181.166:8080/p.html?n=v&m=w
2
IP address

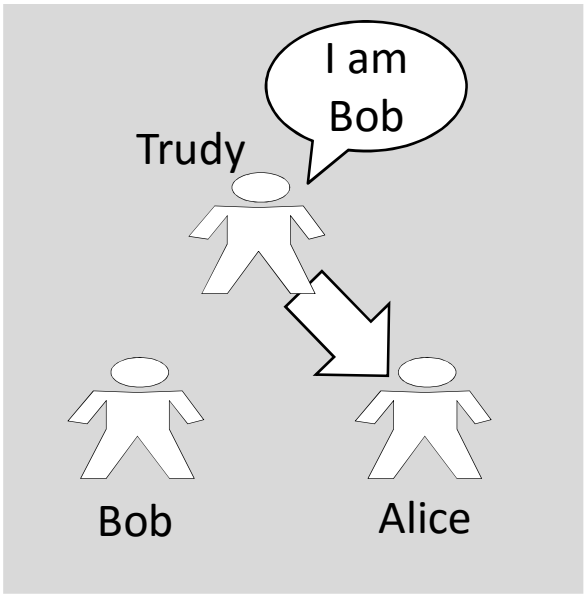

OSI Layer
HTTP request
http://mysite/p.html?n=v&m=w
7
DNS
HTTP request
3
TCP port
http://90.191.181.166:8080/p.html?n=v&m=w
2
IP address

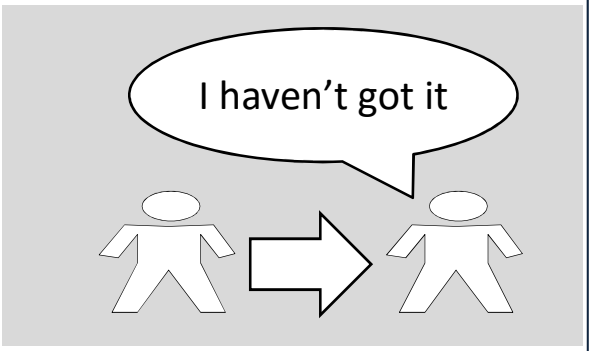
Aspects of Cryptography

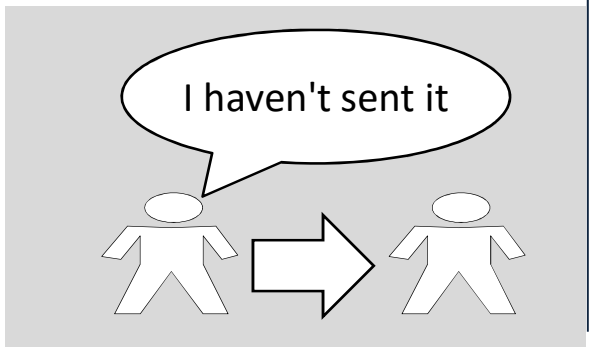
Large-Scale Systems Group
Tallinn University of Technology

- Secrecy
- Forgery Security
- Non-Repudiation



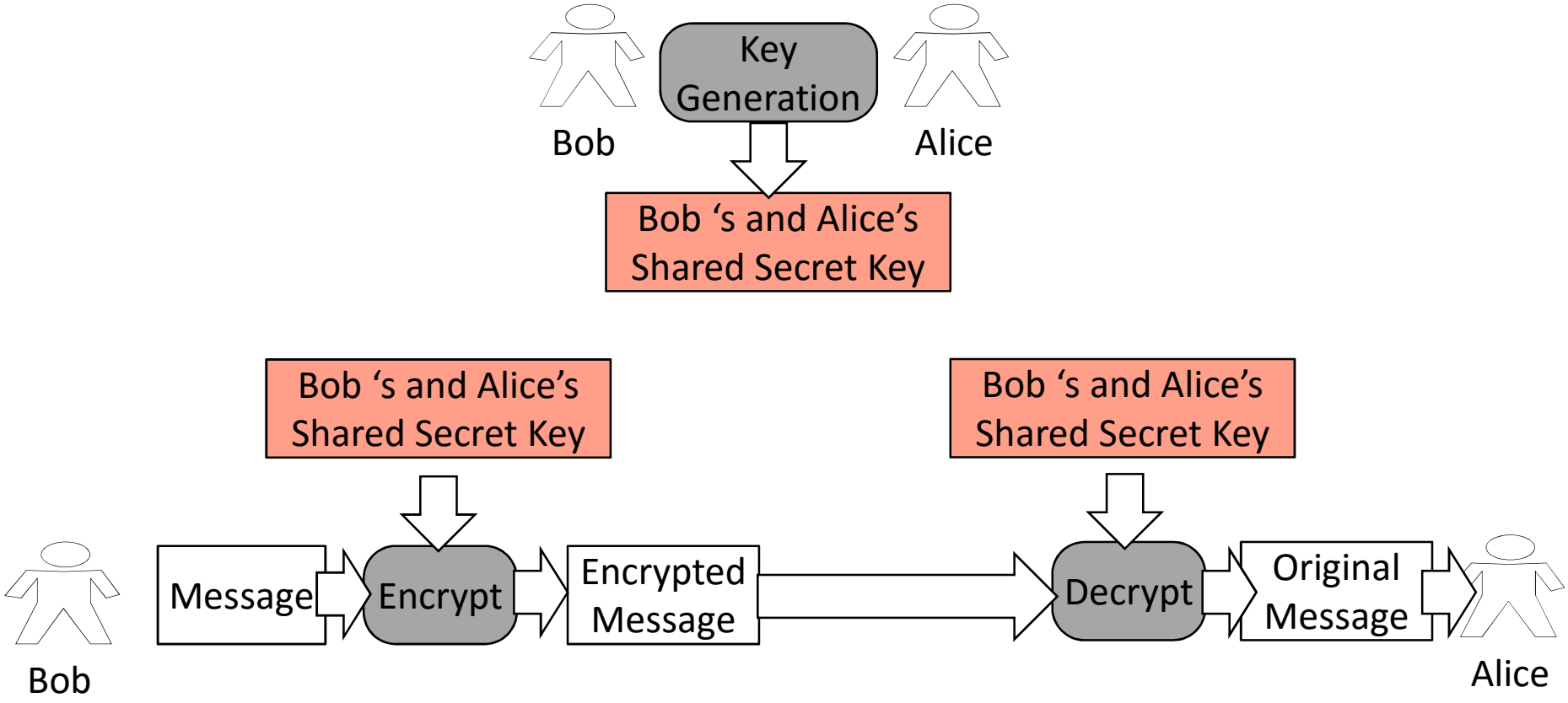






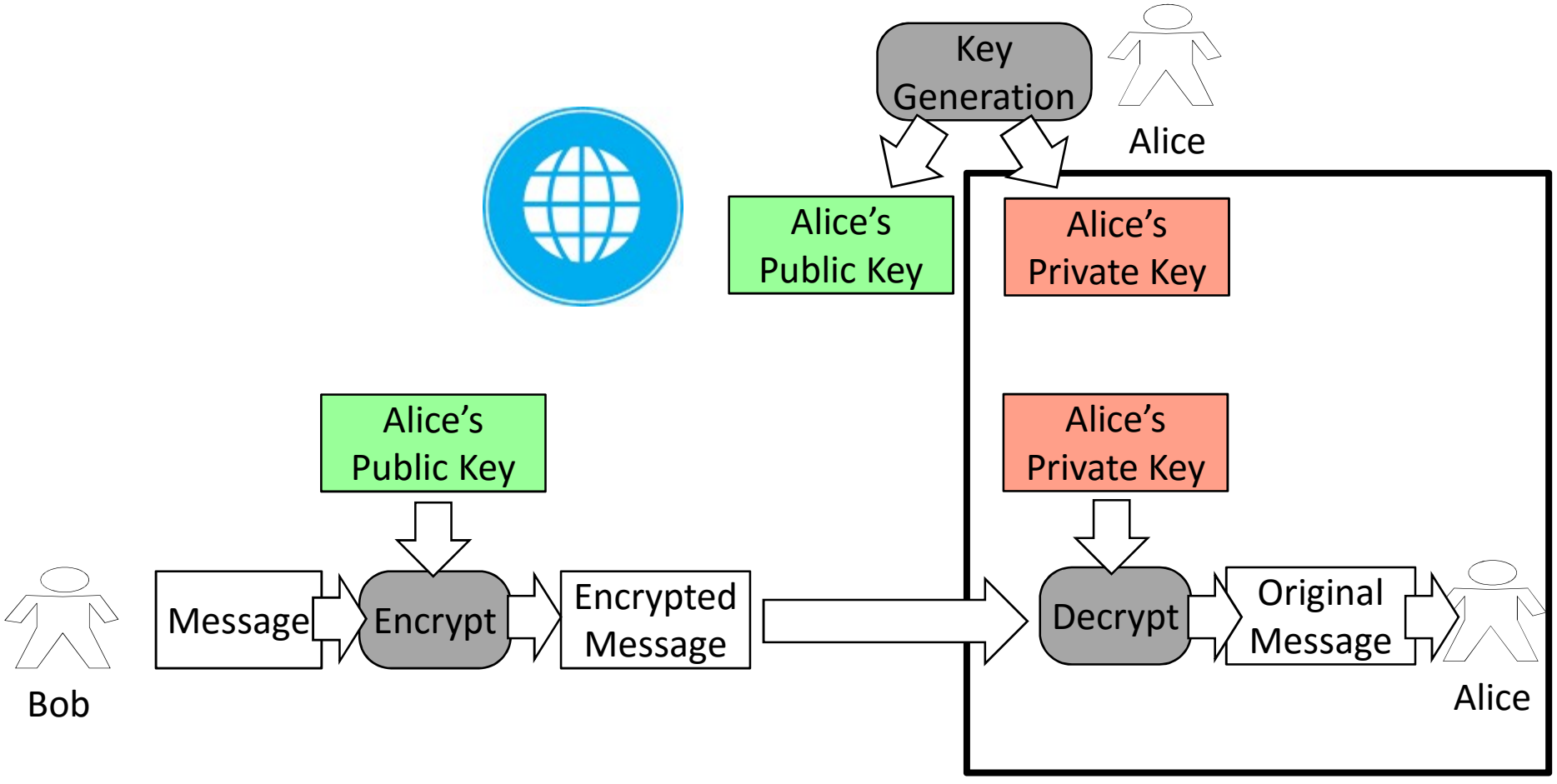
Symmetric Cryptography

Large-Scale Systems Group
Tallinn University of Technology



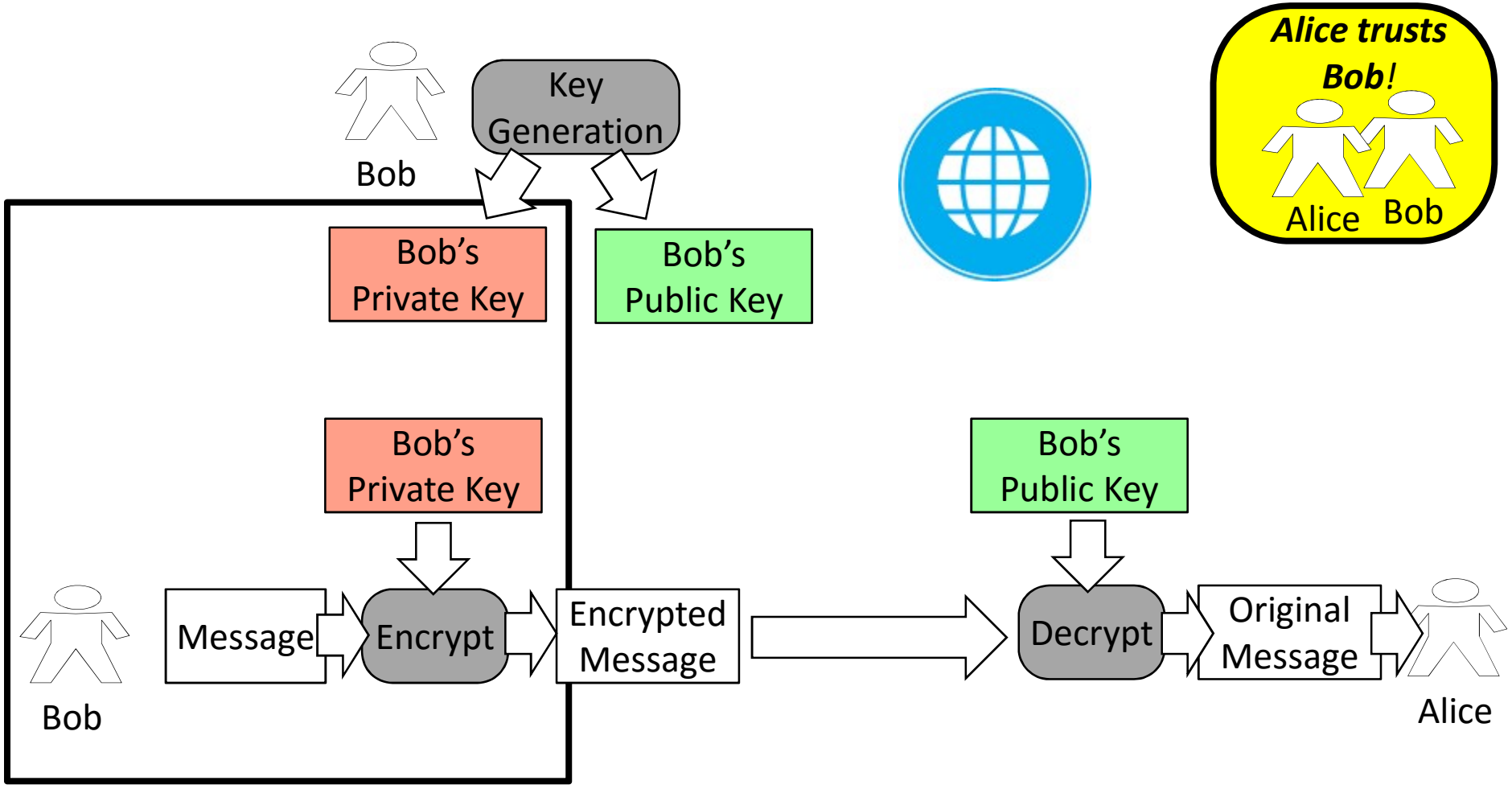
Asymmetric Secrecy

Large-Scale Systems Group
Tallinn University of Technology



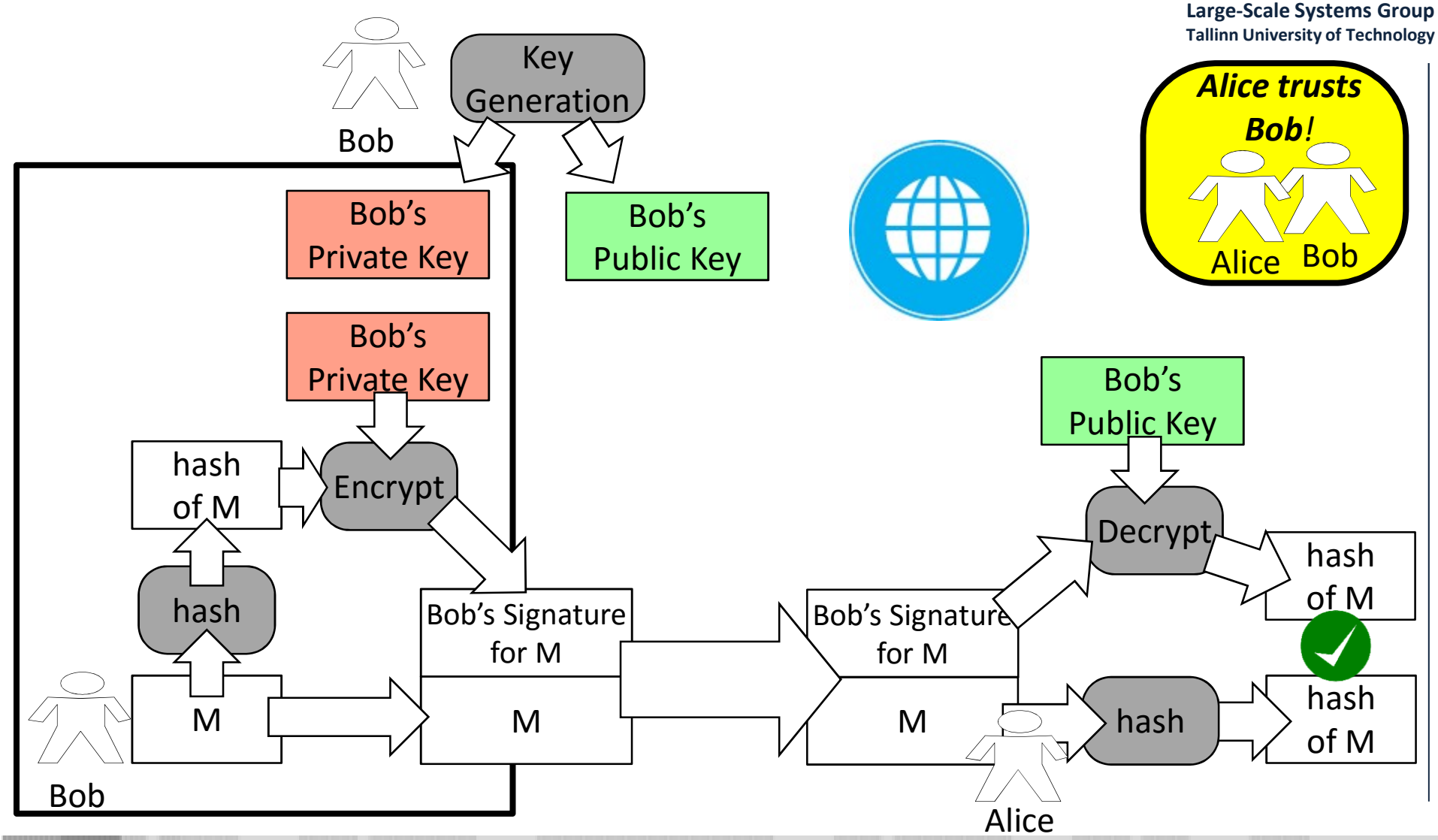
Untrusted Authentication

Large-Scale Systems Group
Tallinn University of Technology



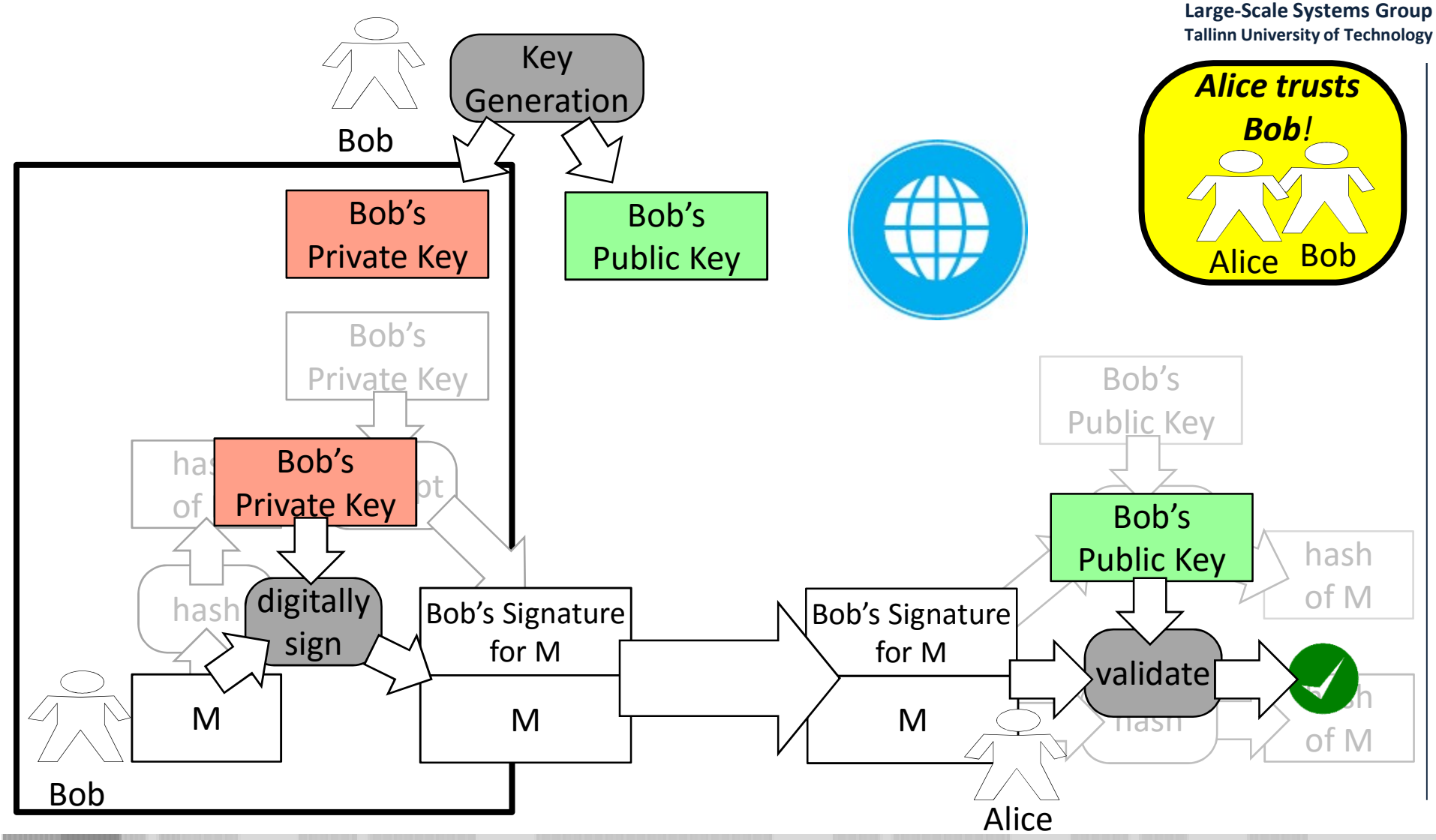
Untrusted Authentication

Large-Scale Systems Group
Tallinn University of Technology

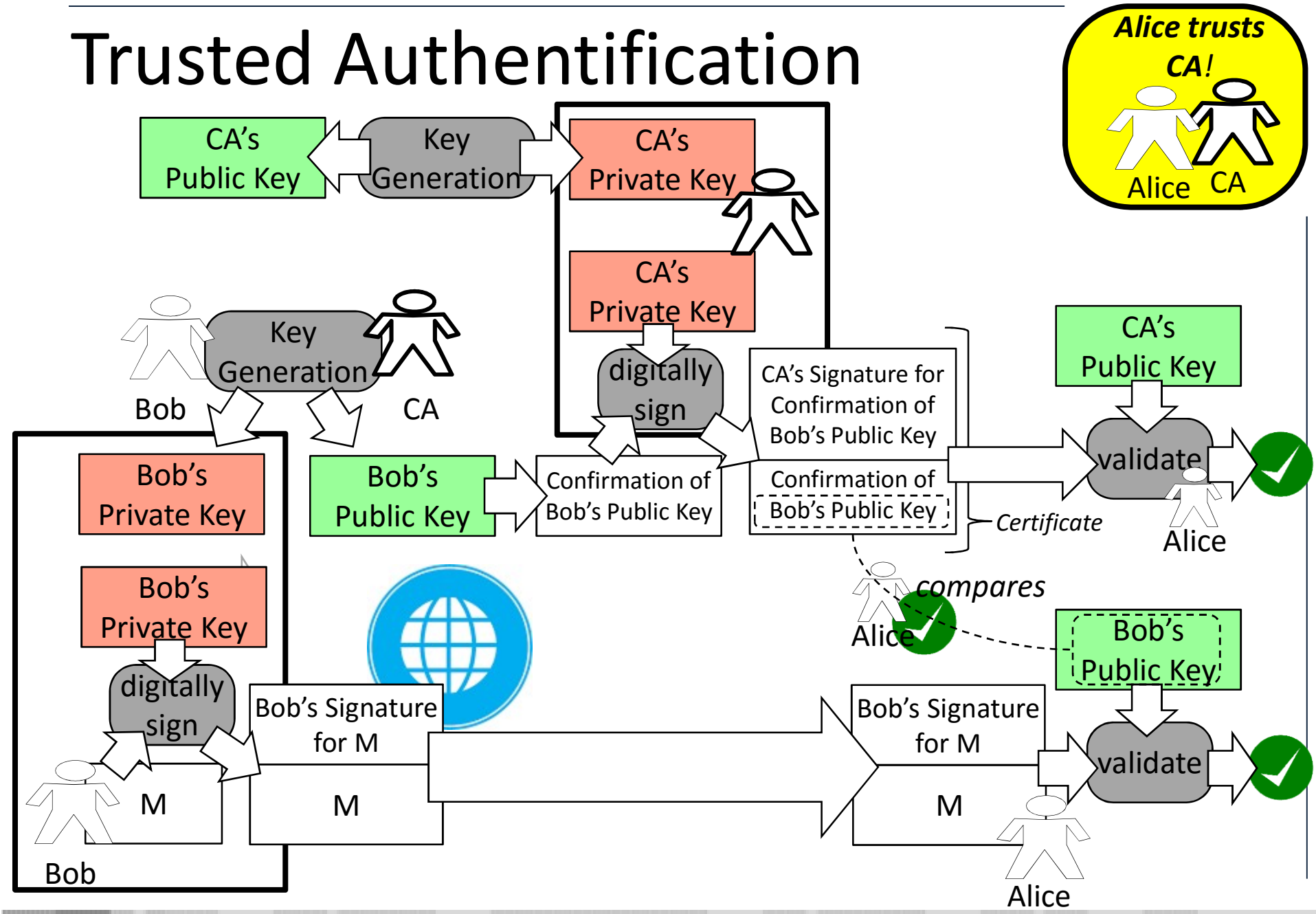


Untrusted Authentication

Large-Scale Systems Group
Tallinn University of Technology



Trusted Authentification



Hybrid Cryptography

Large-Scale Systems Group
Tallinn University of Technology