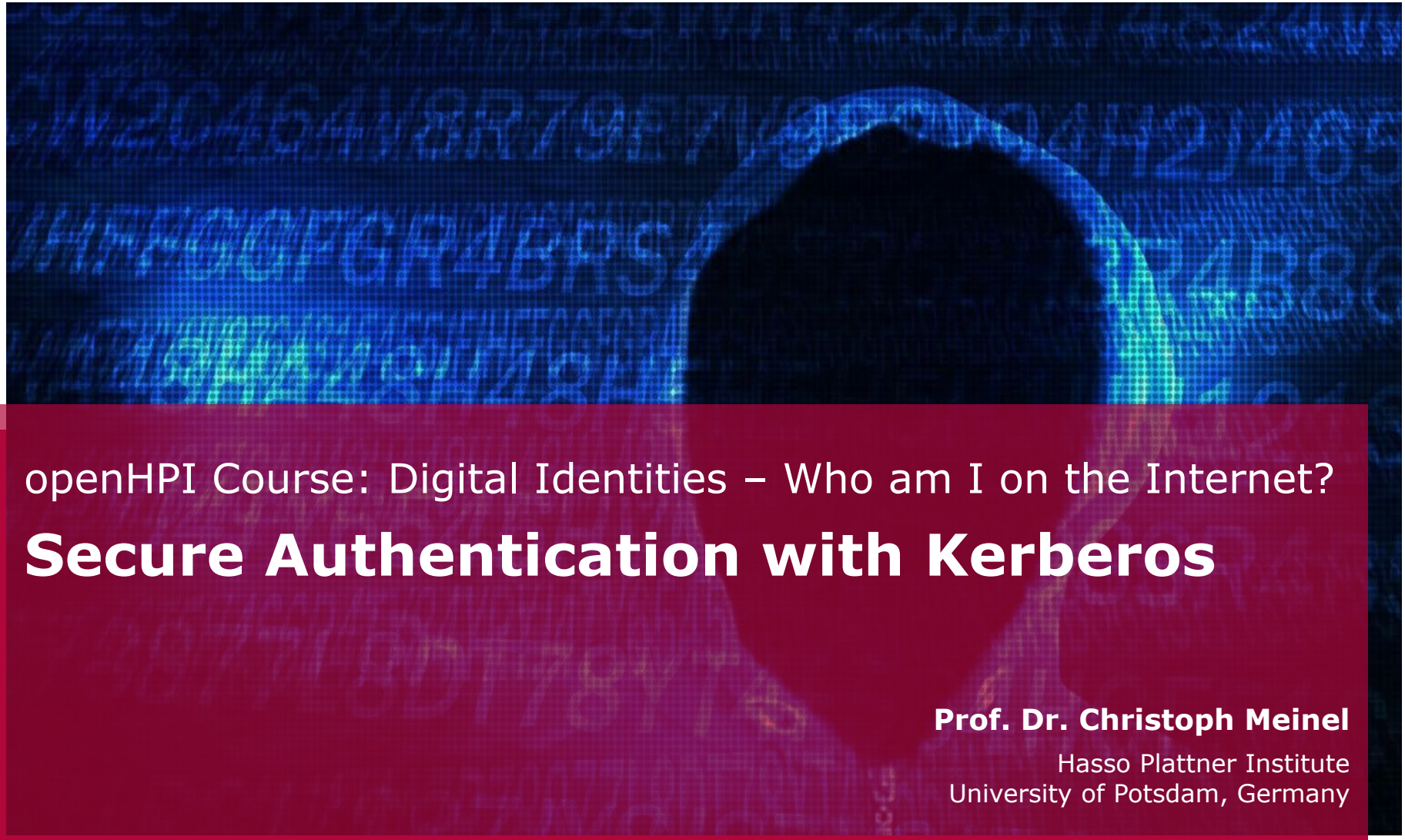


openHPI Course: Digital Identities – Who am I on the Internet?

Secure Authentication with Kerberos

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Kerberos Protocol for Central Authentication

So far we have looked at different models for digital identities. Now we are going to focus on the technical implementation of the models

- We start with the description of the **Kerberos protocol**
- Kerberos is **one of the first authentication protocols** for central authentication
  - there's only one ID provider
  - the various online services trust this ID provider

How does Kerberos work?

- How do online services interact with Kerberos?
- How can online services recognize their users without their own authentication?

Kerberos Protocol for Central Authentication
Terminology

Basic principle: Kerberos protocol issues **tickets**

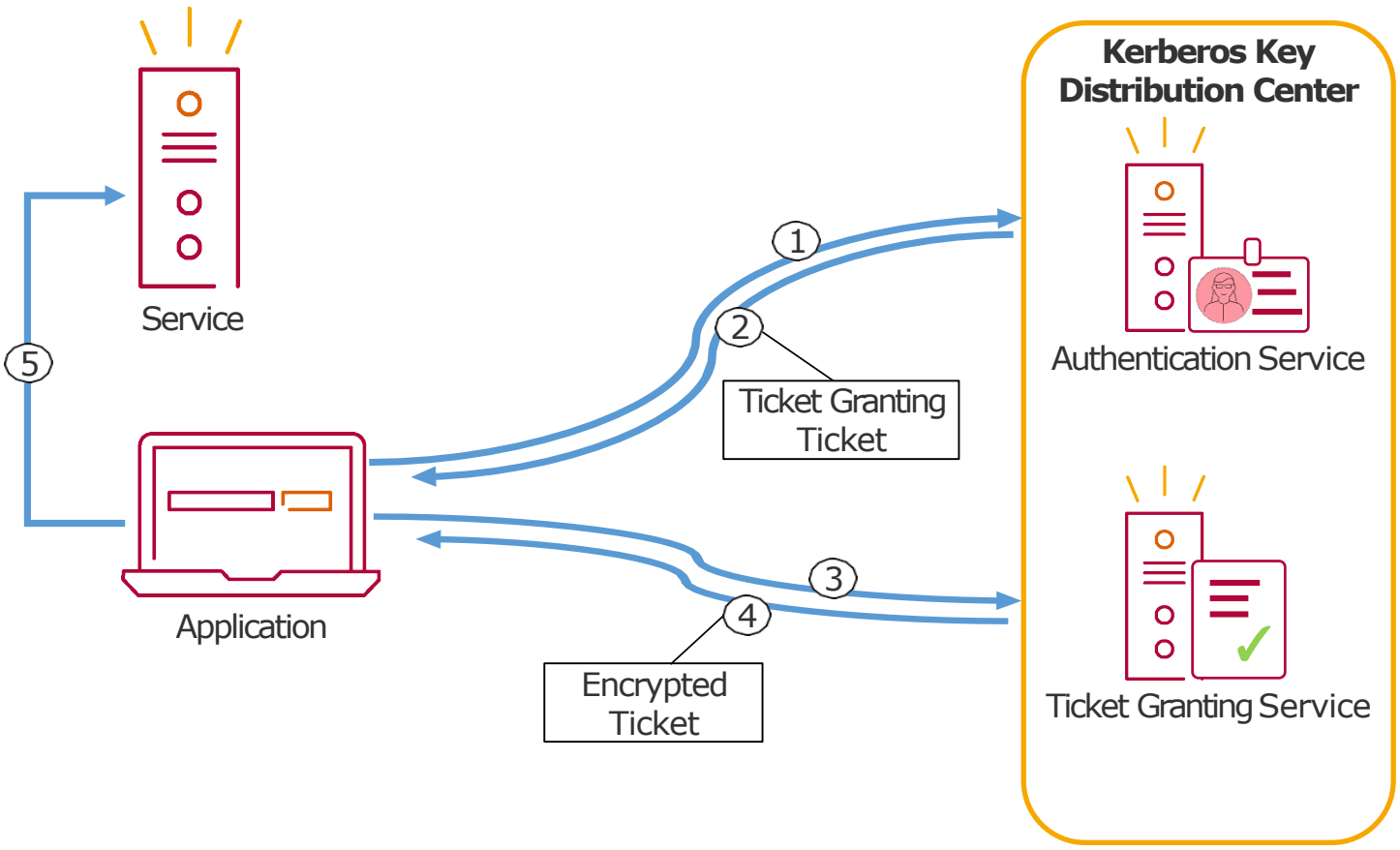
For Kerberos, the ID provider consists of two components:

- Authentication Service
- Ticket Issuing Service (Ticket Granting Service, TGS)

There are **two types of tickets**

- One Master Ticket (Ticket Granting Ticket, TGT)
- Single tickets, valid for only one service

Kerberos Protocol for Central Authentication
Schematic Process



Kerberos Protocol for Central Authentication
Step-by-Step Procedure

1. Authentification with the **Authentication Service**
2. After successful authentication, the user receives a **Master Ticket** (Ticket Granting Ticket, TGT)
3. With this Master Ticket, **single tickets** for the corresponding services can be obtained from the **Ticket Granting Service**
4. Single ticket is encrypted and only valid for one service
5. Single ticket grants **access to the corresponding service**
   - ticket contains an internal ID which is stored by the service to recognize the user
   - to use a second service, a new single ticket for this service can be obtained with the master ticket (without renewed authentication)

Kerberos Protocol for Central Authentication
Advantages and Disadvantages

Advantages:

- One-time authentication is sufficient – the services can be used as long as the master ticket is valid
- Authentication is mutual
  - both user and authentication service make sure that the other partner is in fact the one they claim to be

Disadvantages:

- Single point of failure
- If authentication service (server) is compromised, attacker can imitate any person registered with this service
- Strict synchronization requirements, i.e. all participants must have simultaneous system clocks

Kerberos Protocol for Central Authentication **Applications**

Kerberos protocol is widely used in Windows networks of enterprises and organizations

- Upon joining the company/organization, each employee receives an account, i.e. a digital identity
- With this identity, the employee can log on to any company computer (authentication)
- Automatically and unnoticed he gets a Master Ticket
- If the employee starts Outlook, for example, his personal email account is automatically loaded

Kerberos Protocol for Central Authentication
Summary

Kerberos

- A very popular protocol for **central authentication model**
- Based on **ticket issuance**
- Kerberos ID providers consist of two components
  - **authentication service**
  - **ticket issuing service**
- A **Master Ticket** is issued as result of the authentication
- With the Master Ticket single tickets for the corresponding services can be purchased