



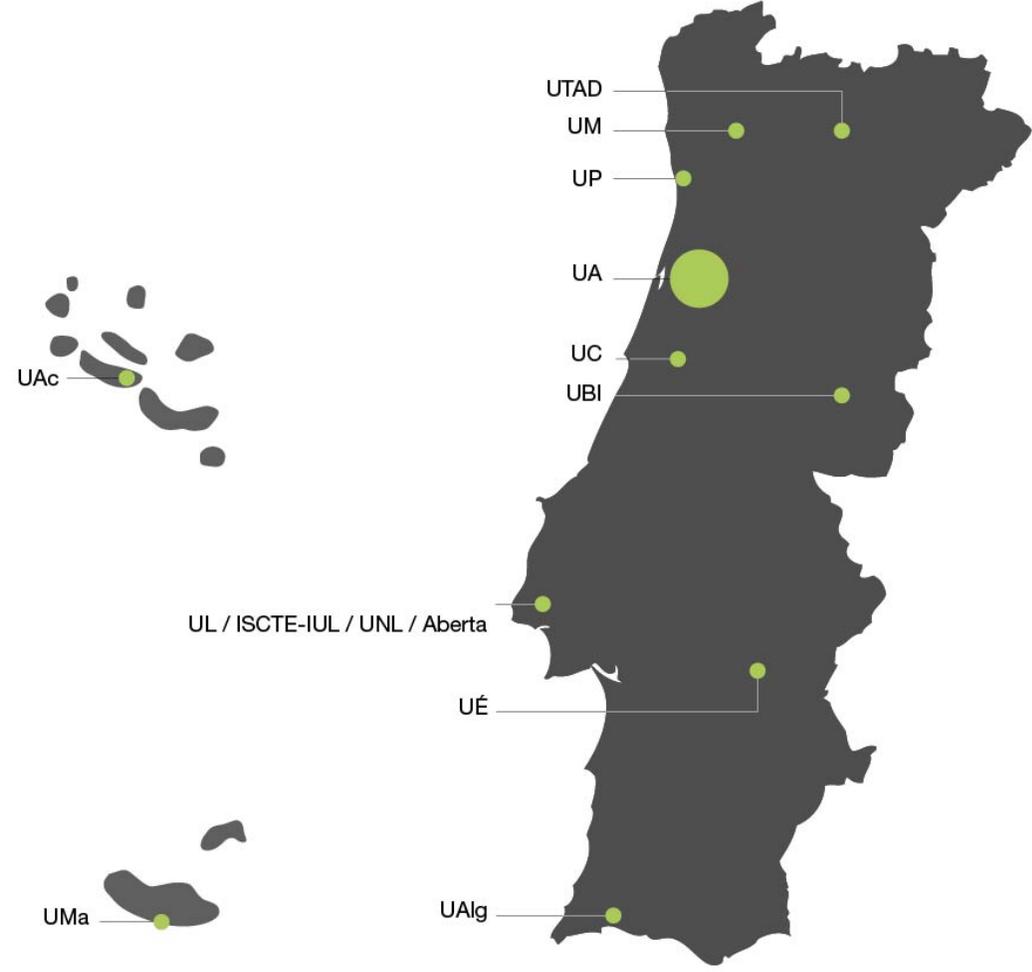
autenTIC @ UA: Autenticação com CMD

Ricardo T. Martins | ricardo@ua.pt | 2018-05-17



Agenda

- A Universidade de Aveiro
- Os sistemas de gestão de identidades e autenticação
- A operação SAMA2020/autenTIC@UA



Um *Campus* que Pensa[®] Um *Campus* que Sente[®] portugal



Um *Campus* que Pensa[®]
Um *Campus* que Sente[®]
portugal





uma grande comunidade



13380

estudantes

5080

em pós-graduação



970

docentes



125

investigadores



365

pós-doc



630

não docentes



88

nacionalidades
(*campus*)



488000

(11500 obras online)



1100

camas



6

cantinas



▪ jovem (1973), pioneira na oferta formativa

- telecomunicações, formação integrada de professores, engenharia cerâmica, engenharia do ambiente, planeamento regional e urbano, engenharia e gestão industrial, turismo, música... foram inovações a nível nacional

▪ sistema binário (2017/2018)

- ensino universitário: licenciaturas de 1º ciclo (25), mestrados integrados (11), mestrados de 2º ciclo (61) e programas doutorais (50)
- ensino politécnico: licenciaturas de 1º ciclo (19) e mestrados de 2º ciclo (6)
- formação não conferente de grau: cursos de formação avançada (1) e cursos de técnicos superiores profissionais (14)



com uma organização singular

sem faculdades

16 departamentos

engenharia

- eletrónica, telecomunicações e informática
- ambiente e ordenamento
- materiais e cerâmica
- mecânica
- civil

artes e humanidades

- línguas e culturas
- comunicação e arte
- educação e psicologia

ciências

- química
- matemática
- geociências
- física
- biologia

ciências sociais

- ciências sociais, políticas e do território
- economia, gestão, engenharia industrial e turismo

saúde

- ciências médicas

4 escolas politécnicas (desde 1997)

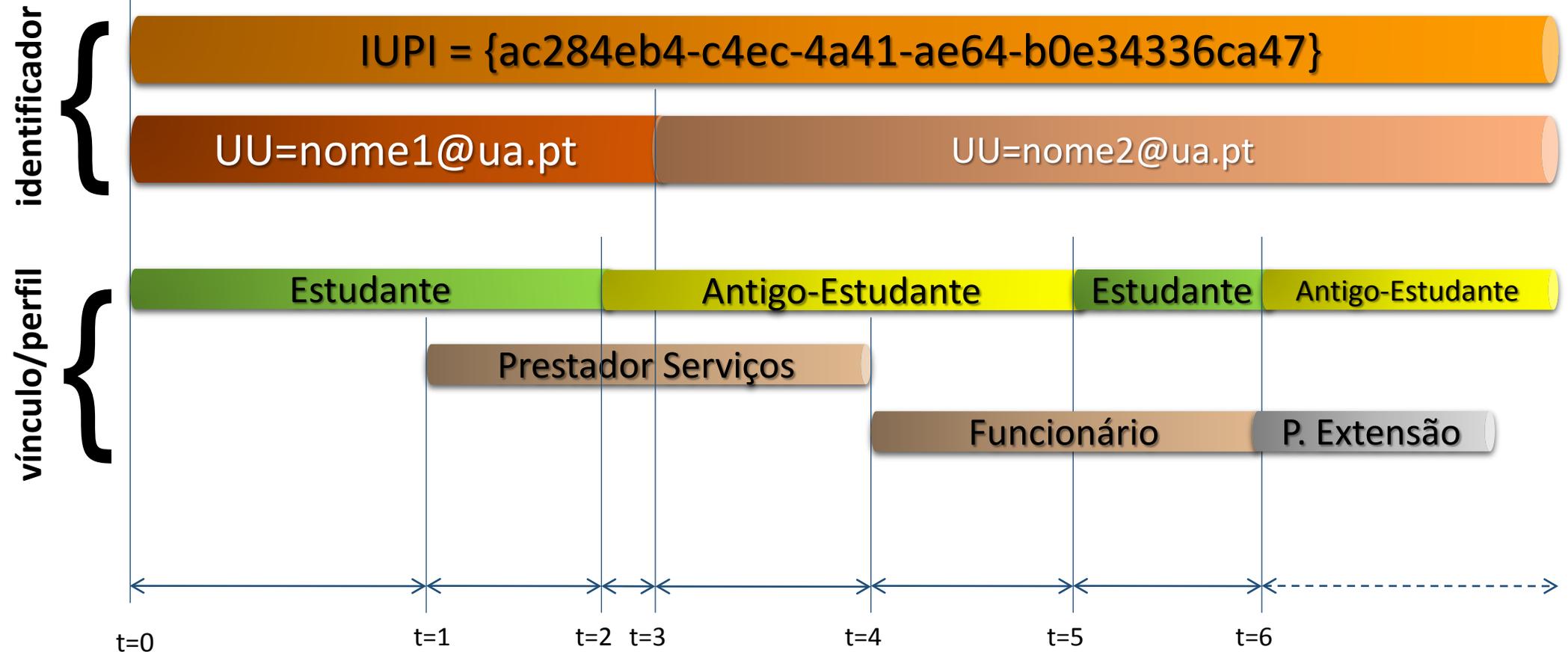
- tecnologia e gestão de água
- contabilidade e administração
- saúde
- design, gestão e tecnologia de produção aveiro norte

Gestão de Identidades na UA

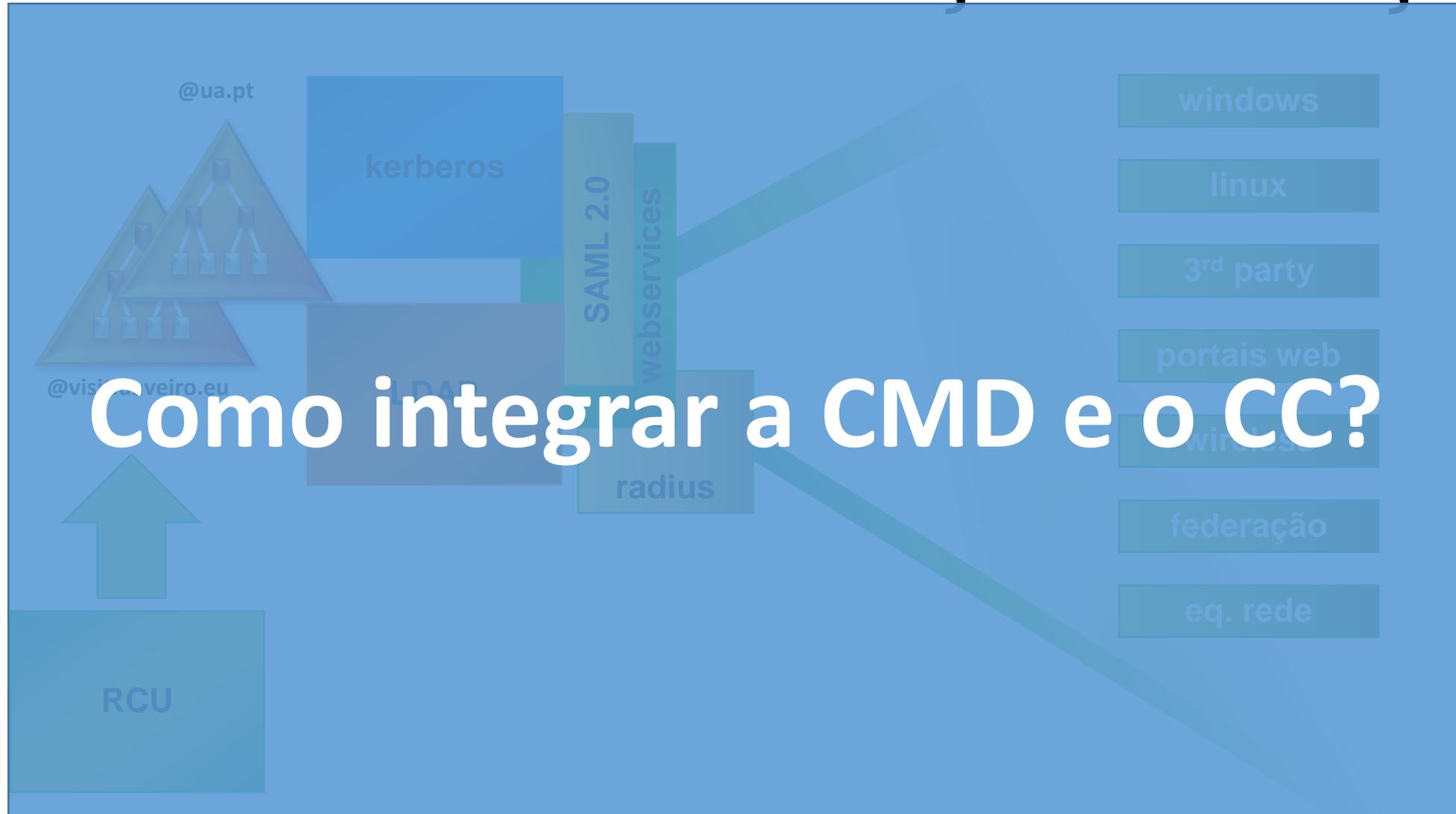
Gestão de Identidades: o caminho percorrido

- 1980's – Múltiplas contas em múltiplos sistemas;
- 2007 – Criação do Utilizador Universal (uma conta, múltiplos sistemas) e o sistema de Gestão de Identidades (IdM)
- 2009 – Integração no serviço de Federação RCTSai
- 2010 – Integração com Federação SAPO
- 2012 – Piloto de autenticação (local) com cartão do cidadão
- 2015 – Autenticação com Chave Móvel Digital / Cartão do Cidadão, recorrendo à plataforma AMA (operação SAM2020/autenTIC@UA)

Gestão de Identidades: modelo



Gestão de Identidades: autenticação e autorização

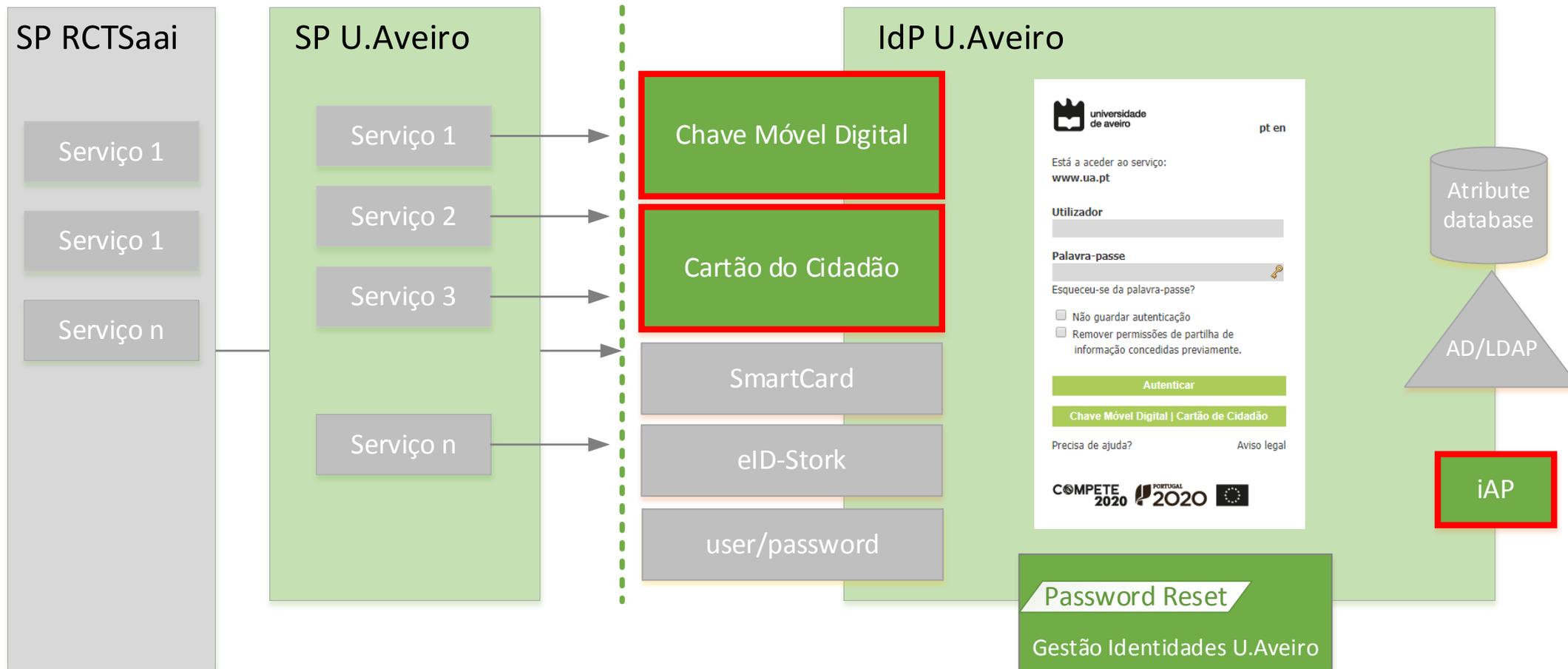


autenTIC @ UA

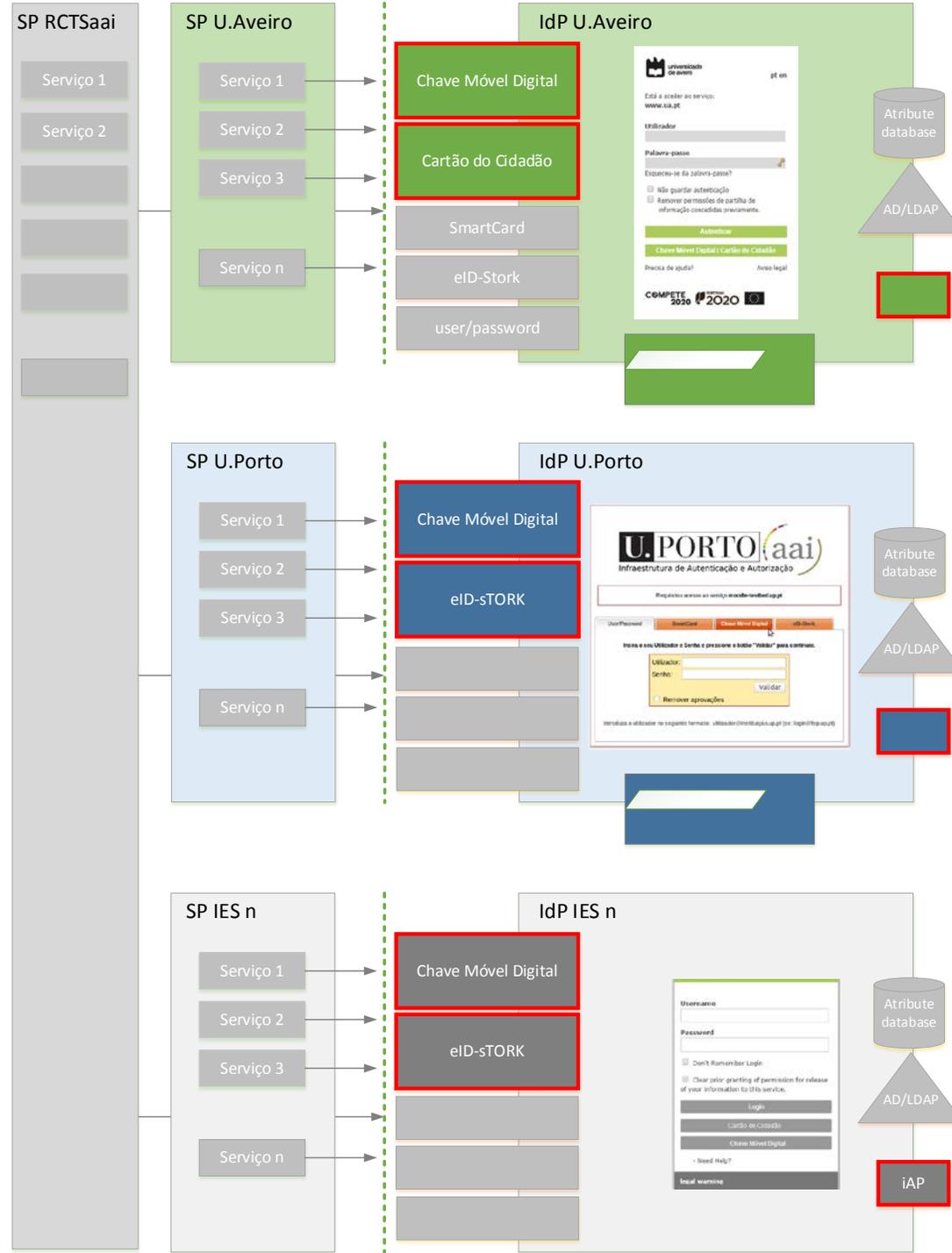
autenTIC: objetivos

- Dotar os serviços das IES com autenticação CMD e CC
- Autenticação CMD segura, acessível e independente para Reset de Password, com integração nos sistemas de IdM
- Autenticação de utilizadores externos às IES com CMD e CC
- Abranger o maior número de serviços → **implementação sobre as infraestruturas AAI (RCTS)**

autenTIC: o modelo concetual



autenTIC: alargado às IES



autenTIC: o cenário

- Projetos financiados SAMA – UAveiro e UPorto
 - 01/SAMA2020/2015 - Operação temática 3: Promover a prestação de serviços eletrónicos com a utilização da Autenticação Eletrónica
 - submissão e aprovação independentes
- Integração de serviços com a autenticação via Chave Móvel Digital (autenticação.gov)
- UAveiro e UPorto partilham da mesma visão – Integração CMD com Autenticação Federada -> Consórcio
- Investimento, Requisitos e Implementação conjunta
- Código Opensource e aplicável às Instituições de Ensino Superior (IES) na RCTSaai
- Apoio e acompanhamento da FCCN

autenTIC e RCTSaai: requisitos

- Integração com Chave Móvel Digital e Cartão de Cidadão
 - integração com Identity Provider (IdP) Shibboleth versão 3.2 ou superior;
 - a integração sem alteração do código base do IdP;
 - a resolução e a libertação de atributos SAML incluídas no fluxo de autenticação/autorização Shibboleth.
 - webflows existentes (default) não alterados para impacto mínimo em futuras atualizações do Shibboleth IdP;
 - libertar, para o Service Provider (SP), um atributo específico com indicação do tipo de autenticação (CMD/CC);
 - Disponibilização de logs para o novo tipo de autenticação;

autenTIC: Interação com a AMA

■ Ambiente de desenvolvimento

- IdP Autenticação.gov administrado pela AMA – Fornecedor de Autenticação (FA);
- processo simples;
- troca de certificados (não self-sign);
- informação para os atributos "Issuer" (nome do servidor SP) e "ProviderName" (nome da Universidade);

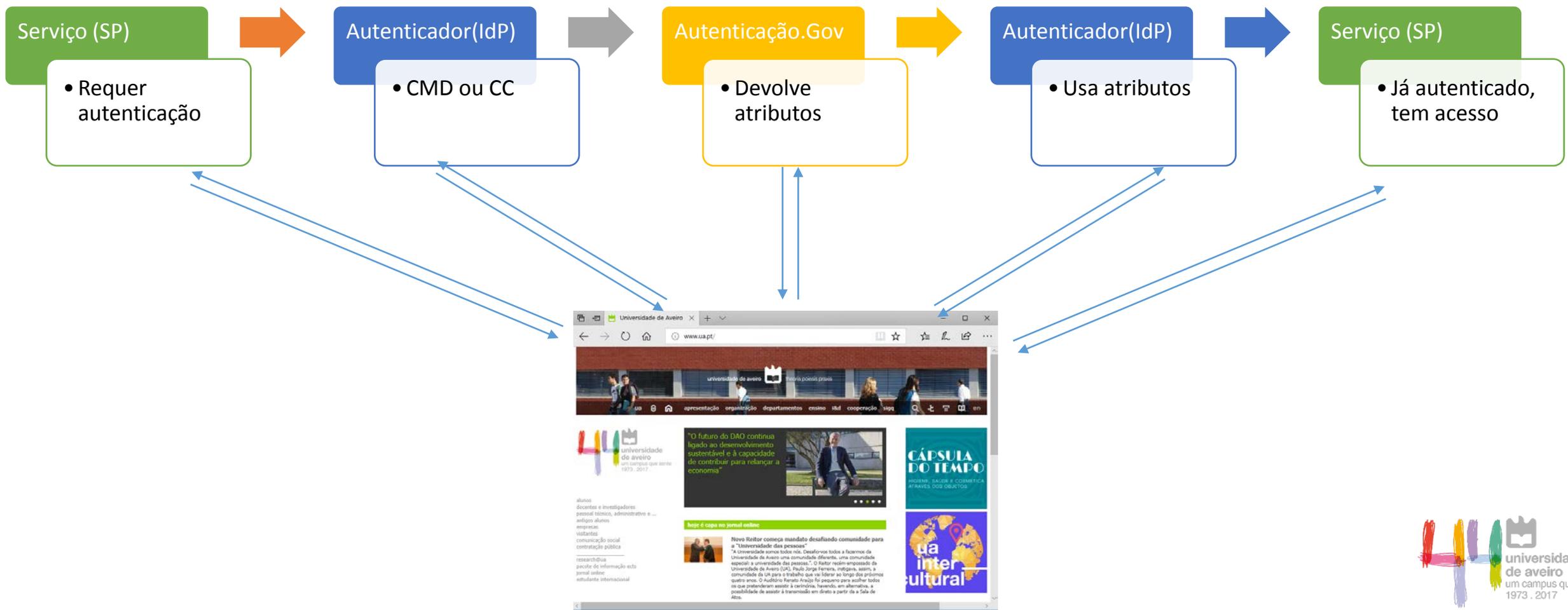
■ Ambiente de produção

- Igual a desenvolvimento + Protocolo AMA/IES.

autenTIC: Desenvolvimento

- Por entidade externa;
- Integração com IdP Shibboleth;
- Construção de *external flows*;
- Servlet Java com configurações XML;
- Estreita colaboração UA/UP/FCT-FCCN

autenTIC: demo



autenTIC: promoção e divulgação

- Foi implementado em 2017
- Foi divulgado nas Jornadas FCCN
- Foi realizado um workshop de implementação nas IES em abr/2018



Autenticação com cartão de cidadão ou chave móvel digital no sistema de informação único da Universidade?



Estudantes, docentes, investigadores e pessoal técnico, administrativo e de gestão da Universidade de Aveiro vão passar a poder aceder ao sistema de informação único da Universidade de forma mais segura. Se até aqui a autenticação era feita exclusivamente via login com a conta institucional (o tradicional utilizador e password), a partir deste verão o acesso vai passar a poder ser feito também via cartão de cidadão ou chave móvel digital.

A chave móvel digital (CMD) é um meio alternativo que permite a autenticação e acesso a serviços em portais e sítios na internet com recurso ao telemóvel, email ou Twitter. Tal é possível através da associação do número de telemóvel, email ou Twitter ao número de identificação civil (NIC) para um cidadão português, ou ao número de passaporte para um cidadão estrangeiro residente em Portugal.

Trata-se de um método de autenticação simples (uma senha para todos os sítios), mais seguro (código enviado por SMS, email ou Twitter).

Objetivos e vantagens associadas:

- ✓ Recorrer à autenticação multifator em aplicações mais sensíveis;
- ✓ Efetuar a reposição da password sem intervenção dos STIC, com recurso ao cartão de cidadão, chave móvel digital, pin telefónico e/ou email alternativo;
- ✓ Efetuar logout de forma segura em todas as aplicações a que o utilizador tenha acedido, recorrendo à autenticação federada;
- ✓ Utilizadores estrangeiros podem autenticar-se de forma segura, com recurso à chave móvel digital.

Agradecimentos

- À AMA (equipa tecnológica e equipa de gestão de projeto)
- À FCT/FCCN
- À Universidade do Porto

Questões?