

Mestrado em Engenharia Informática (MEI)

Mestrado Integrado em Engenharia Informática

(MiEI)

Perfil de Especialização **CSI** : Criptografia e Segurança da Informação

Engenharia de Segurança



Tópicos

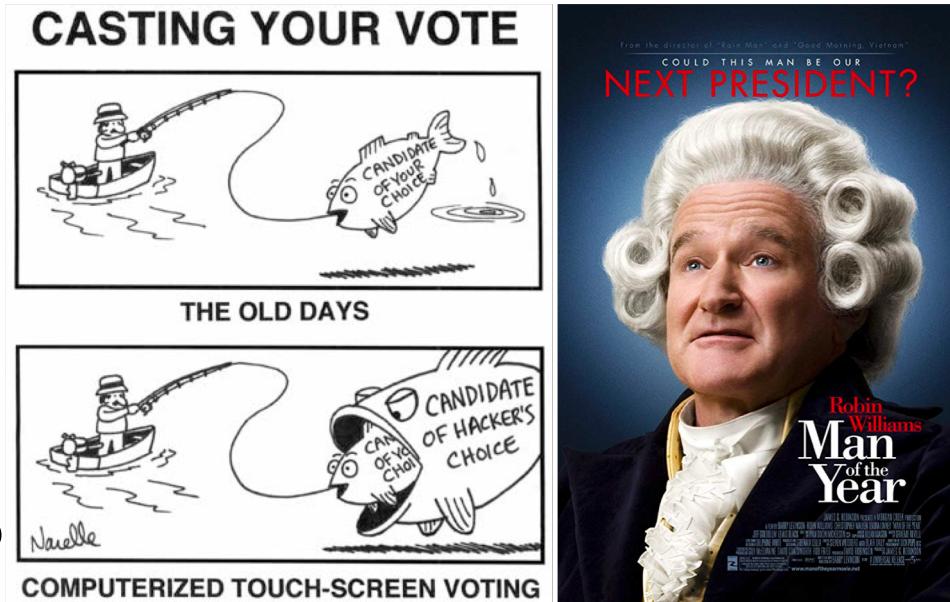
- Criptografia Aplicada
 - Protocolos/aplicações criptográficas
 - Voto eletrónico



Voto Electrónico

- Protocolo de votação em rede aberta, com as seguintes **garantias gerais**:

- Autenticação do Eleitor
- Anonimato do Eleitor
- Confidencialidade do Voto
- Integridade do Voto
- Não extravio do Voto
- Integridade do sistema de Voto
- Auditabilidade do sistema de Voto



- O protocolo dos exemplos apresentados assume que os votantes não dispõem de meios de identificação avançados (como por exemplo, certificado digital pessoal) nem são peritos tecnológicos.

Voto Electrónico – Exemplo 1

- **Entidades** participantes no Voto Electrónico:
 - Promotor: A entidade que promove a votação;
 - SMV (Sistema de Mediação de Votos): plataforma de votação (*frontend* e *backend*) responsável por gerir e processar os votos electrónicos durante o período de votação, findo o qual os fará chegar ao Promotor;
 - Votante: O indivíduo que pretende exercer o seu direito de voto, escolhendo as opções existentes, conforme política do boletim de voto (para efeitos do protocolo, voto branco e voto nulo podem ser vistos como opções adicionais que o Promotor pode ou não activar);
 - Auditor: Indivíduo/Entidade que acompanha o processo de votação, podendo comprovar a correcção deste sem tomar conhecimento sobre o sentido de voto de cada um dos participantes.

Voto Electrónico – Exemplo 1

- Com este protocolo de Voto electrónico pretende-se:
 - O **Votante** possa aceder a interface Web ou app de votação que, após lhe mostrar as opções existentes e solicitar a introdução dos elementos de autenticação necessários, lhe permita votar e obter uma prova de como efectuou a votação dentro do prazo estipulado;
 - O Votante possa provar a existência de situações de rejeição fraudulenta de votos efectuados dentro do prazo estabelecido;
 - O Votante possa proteger-se do facto de, embora tenha efectuado o seu voto dentro do período da votação, o servidor apenas o tenha processado após este período ter terminado;
 - O **SMV** não tome conhecimento do conteúdo dos votos;
 - O SMV não possa alterar o conteúdo dos votos sem que isso seja detectado pelo Promotor;
 - O SMV não possa alterar o número de votos sem que isso seja detectado pelo Promotor;
 - O **Promotor** não tome conhecimento do conteúdo dos votos até ao final da eleição;
 - O Promotor não possa alterar o conteúdo dos votos sem que isso seja detectado pelo SMV;
 - O Promotor não possa alterar o número de votos sem que isso seja detectado pelo SMV;
 - O Promotor receba, de forma segura, os votos (cifrados com a chave pública do Promotor) efectuados durante o período de votação, juntamente com um comprovativo do instante temporal em que deram entrada no SMV;
 - O Promotor se possa defender de suspeitas infundadas de rejeição de votos efectuados dentro do prazo estabelecido;
 - O Promotor possa ter a certeza que durante o período da votação ninguém toma conhecimento do conteúdo dos votos;
 - **Nenhum interveniente** no processo consiga saber quem votou o quê.



Voto Electrónico – Exemplo 1

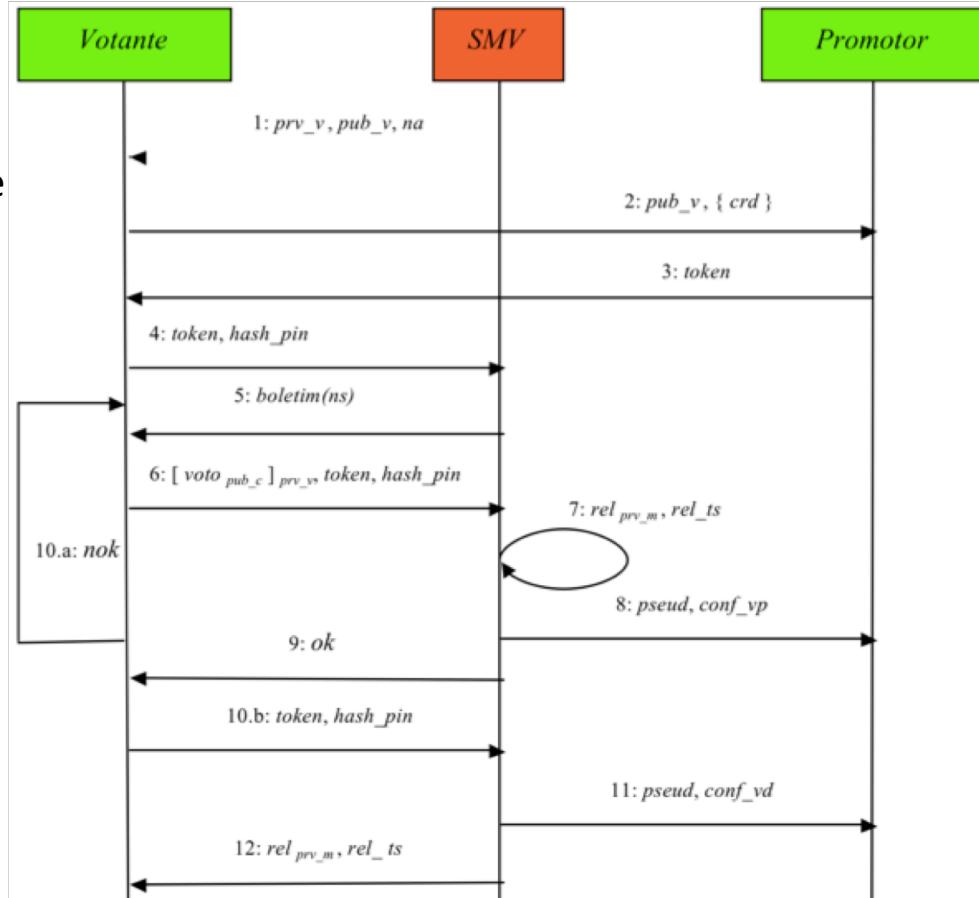
- Preparação do Voto electrónico (**fase pré-voto**):
 - O **Promotor** comunica ao SMV:
 - Grupo de votantes, período de votação, boletins de voto e possibilidades de voto de cada boletim (política do boletim de voto).
 - Identificação dos votantes e contactos, de modo ao SMV enviar credenciais de autenticação de votação (por exemplo, número de identificação do votante perante o Promotor e PIN gerada pelo SMV);
 - O **Promotor** indica ao SMV que tipo de credencial adicional de autenticação deve ser pedido ao Votante de modo ao Promotor a conseguir validar (por exemplo, número de identificação do votante perante o Promotor e data de nascimento);
 - O Promotor gera um par de chaves e o respectivo certificado de votação, fornecendo o certificado ao SMV;
 - O Promotor gera um par de chaves e o respectivo certificado de assinatura, fornecendo o certificado ao SMV;
 - O Promotor gera um par de chaves e o respectivo certificado para cifra dos votos, fornecendo o certificado ao SMV;
 - O Promotor disponibiliza um Web service HTTPS que, recebendo uma chave pública juntamente com as credenciais do Votante (conhecidas pelo Promotor), devolva um token assinado pelo Promotor (utilizando o seu certificado de assinatura) a autorizar a realização do voto.



Voto Electrónico 1 – período de votação

Passo 1:

- O Votante acede ao interface web ou app de votação, cujo endereço lhe foi comunicado pelo Promotor;
- O Votante introduz as credenciais pedidas (umas conhecidas pelo votante e pelo SMV e outras conhecidas pelo votante e pelo Promotor);
- É gerado um par de chaves (*prv_v*, *pub_v*) e um número aleatório *na* para este Votante.



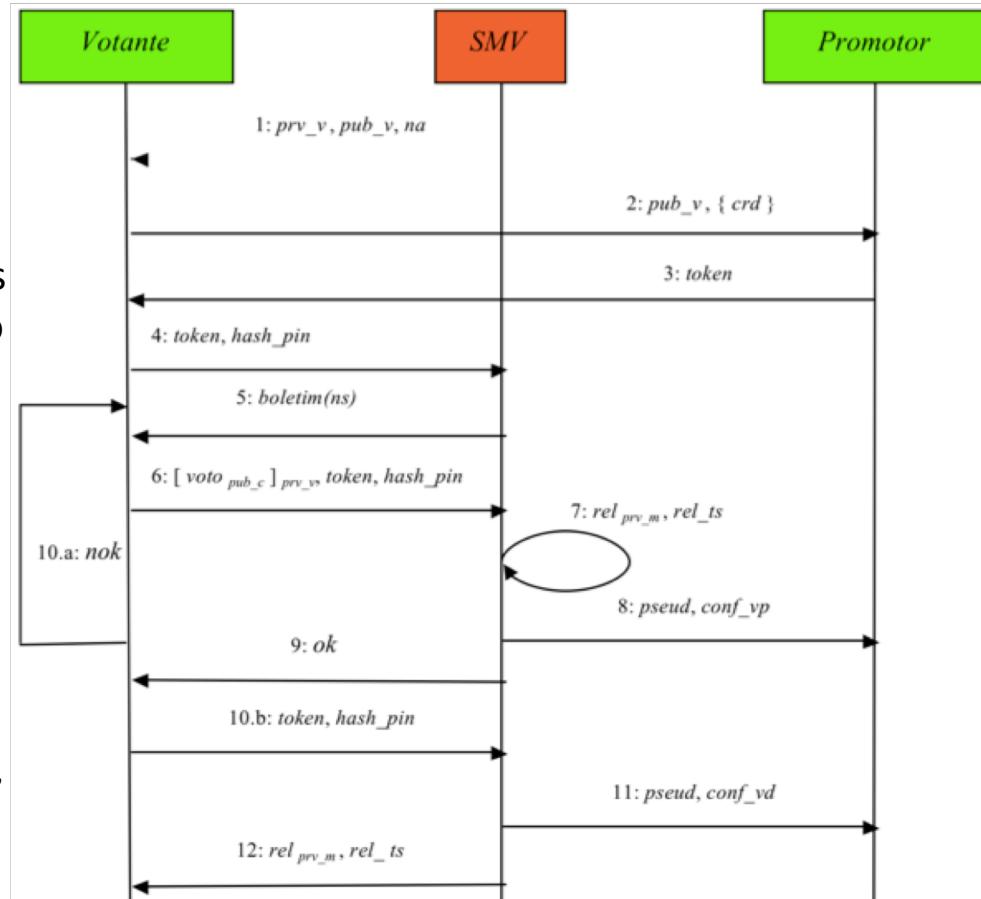
Passo 2:

- O interface web ou app de votação efectua (sem intervenção do Votante) um POST HTTPS para o serviço Web disponibilizada pelo Promotor (validando o serviço pelo certificado de servidor Web), enviando a chave pública gerada (*pub_v*) e as credenciais (conhecidas pelo Votante e pelo Promotor) introduzidas no passo anterior.

Voto Electrónico 1 – período de votação

Passo 3:

- a. Caso as credenciais recebidas estejam correctas, o Promotor devolve um token de autorização assinado por si (com a chave privada de assinatura) que autoriza o Votante a participar na eleição. Deste token é possível extrair o pseudónimo do Votante, o grupo a que pertence o Votante e quais os boletins de voto a que deverá ter acesso, e o número de votos que a sua votação representará, assim como contém a chave pública do votante (*pub_v*).



Passo 4:

- a. O interface web ou app de votação envia (sem intervenção do Votante) o token de votação (recebido do Promotor) para o SMV, juntamente com a hash das credenciais conhecidas entre Votante e SMV (*hash_pin*).

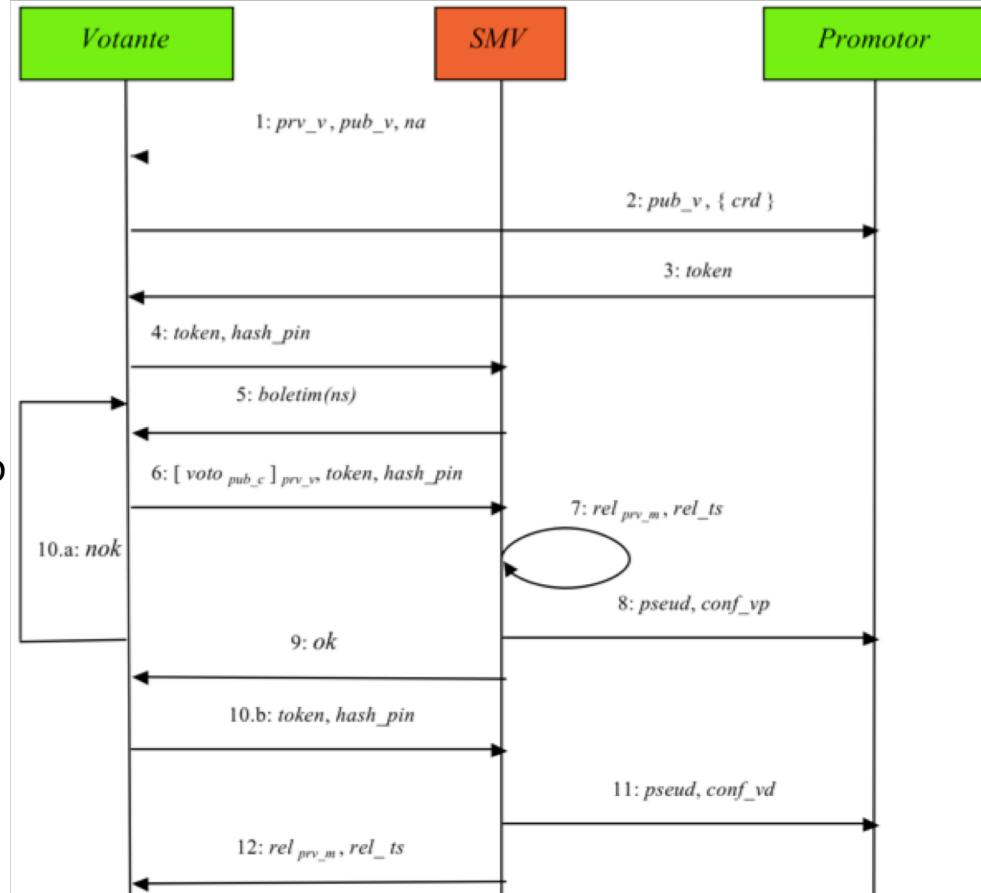
Voto Electrónico 1 – período de votação

Passo 5:

- O SMV indica à interface web/app de votação quais os boletins que o Votante está autorizado a visualizar e preencher;
- O Votante efectua a votação de acordo com a política de cada boletim de Voto.

Passo 6:

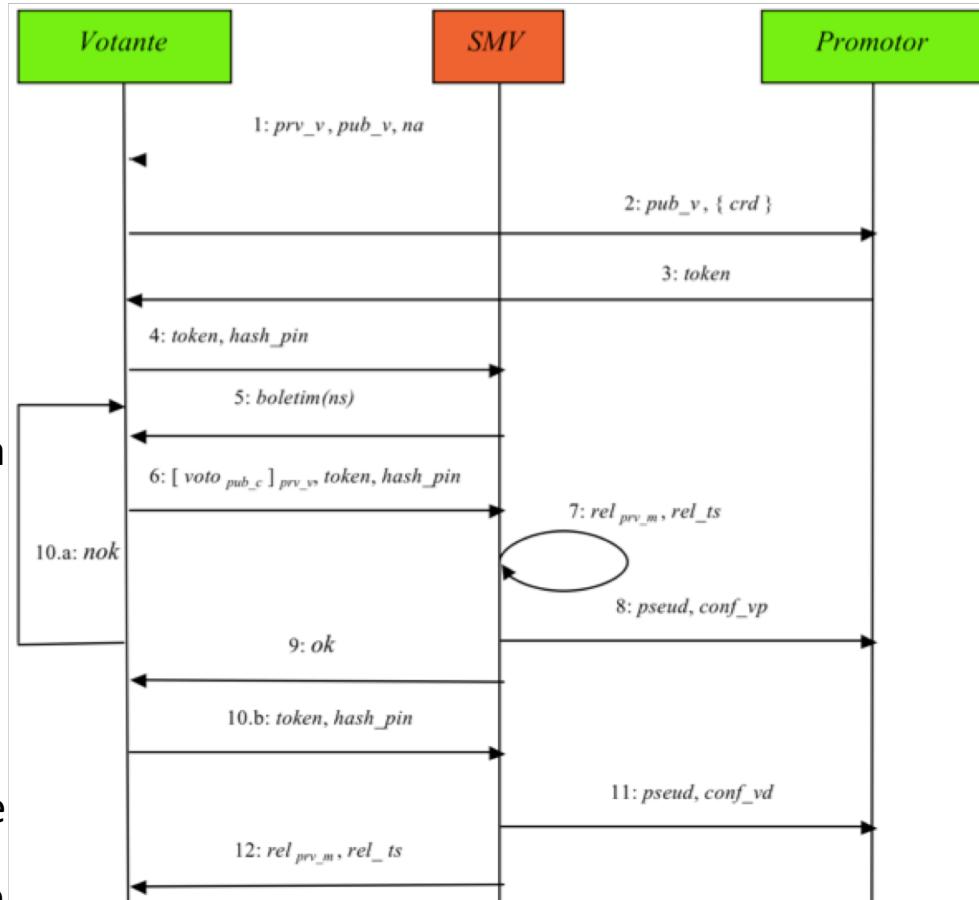
- A interface web/app de votação cria o voto que, para além das opções seleccionadas, inclui também o número aleatório *na* gerado anteriormente, cifrando-o com a chave pública do Promotor (*pub_c*, obtida do certificado de votação do Promotor) e assinando-o com a chave privada *prv_v* do Votante, gerada no primeiro passo.
- A assinatura gerada é enviada ao SMV, juntamente com o token e com a *hash_pin*.



Voto Electrónico 1 – período de votação

Passo 7:

- O SMV verifica se:
 - reconhece o *hash_pin* (*hash_pin* gerados são únicos)
 - o token é válido e,
 - o voto foi assinado com a chave privada (*do votante*) que corresponde à chave pública contida no token.
- O SMV gera um relatório de recepção onde inclui o pseudónimo do Votante *pseud*, assinando-o com a chave privada *prv_m* do SMV, dando origem a *rel_{prv_m}*.
- O SMV obtém um timestamp sobre o relatório assinado, por forma a ter a prova da data/hora legal a que terminou de processar o recebimento do voto, ficando com *rel_ts*.
- Se a data/hora que consta de *rel_ts* se encontrar fora do período da votação, o voto é descartado e é devolvida uma mensagem de erro no passo 9. Caso contrário, o SMV considera o voto válido e armazena-o na sua base de dados, juntamente com o relatório de recepção e respectivo timestamp.



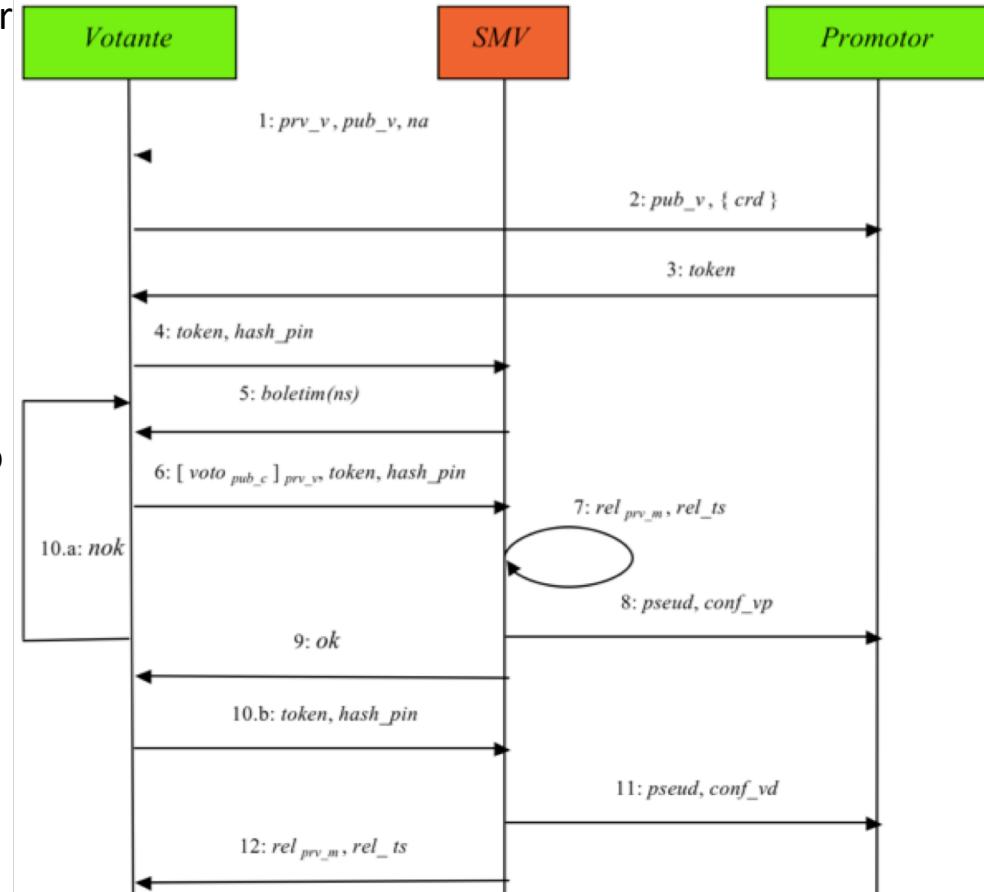
Voto Electrónico 1 – período de votação

Passo 8:

- a. Se as verificações efectuadas no passo anterior forem bem sucedidas é enviado, por POST HTTPS para um serviço Web do Promotor, uma confirmação provisória *conf_vp* de que o Votante com o pseudónimo *pseud* acabou de exercer o seu direito de voto.

Passo 9:

- a. Se as verificações efectuadas no passo 7 não tiverem sido bem sucedidas, é apresentada uma mensagem de erro explicativa ao Votante. Caso contrário, ser-lhe-ão mostradas as escolhas que fez em cada um dos boletins de voto, perguntando-lhe simultaneamente se as deseja confirmar.



Voto Electrónico 1 – período de votação

Passo 10a:

- Caso o Votante pretenda alterar o seu sentido de voto, o processo volta para o passo 5.

Passo 10b:

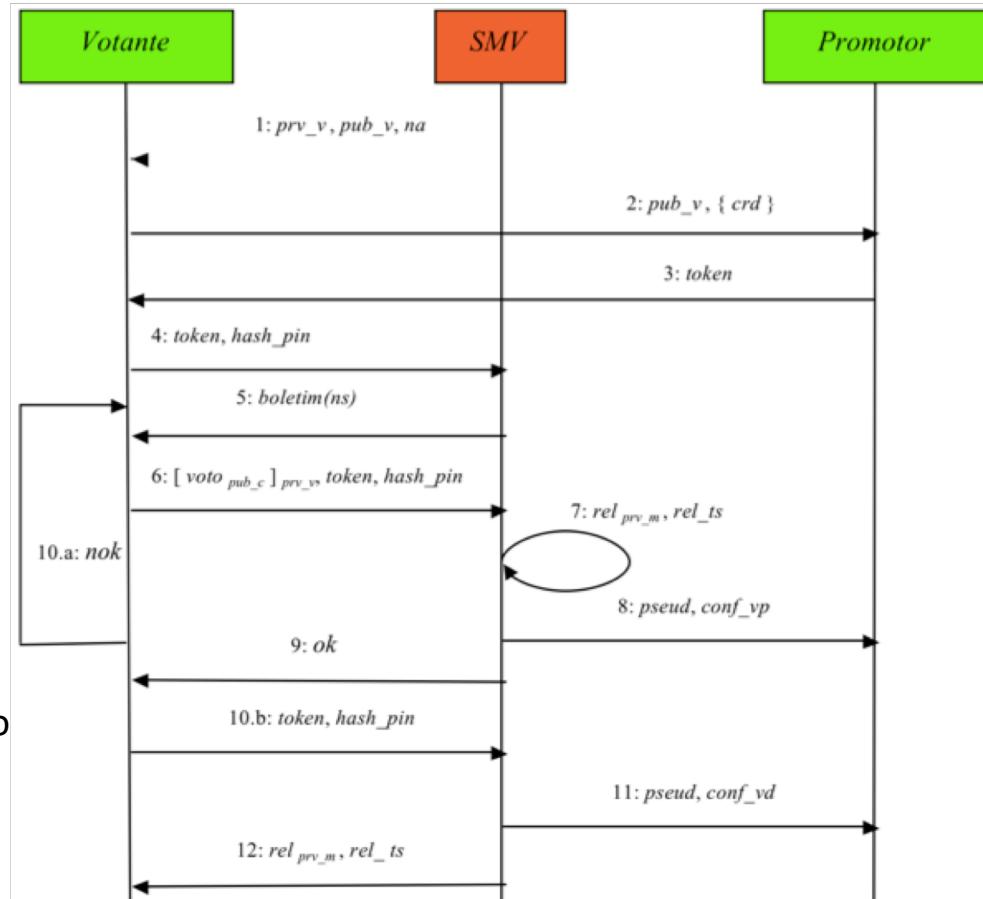
- Caso o Votante pretenda confirmar o seu sentido de voto, o token e a *hash_pin* do Votante são enviados novamente ao SMV, dando o voto como definitivo.

Passo 11:

- O SMV repete o passo 8 só que desta vez é enviada, ao Promotor, uma confirmação definitiva (*conf_vd*) do voto efectuado pelo Votante *pseud*.

Passo 12:

- O relatório de recepção assinado (rel_{prv_m}) e o respectivo time-stamp (rel_ts) gerados no passo 7 são devolvidos ao Votante para que este os possa armazenar como prova (com validade legal) de que exerceu o seu direito de voto dentro do período definido, sem que seja quebrada a confidencialidade do seu voto.



Voto Electrónico – Exemplo 1

- Voto electrónico (**fase pós-voto**):
 - Findo o período de votação, o SMV envia ao Promotor:
 - conjunto de votos (cifrados mas sem a assinatura dos Votantes) assinados pelo SMV – garantindo que o Promotor não sabe quem votou o quê -;
 - relatórios de recepção de votos e os respectivos time-stamps obtidos.
 - O Promotor, com a sua chave privada de votação decifra os votos e efectua a contagem automática dos resultados da votação.
- Com os dados fornecidos pelo SMV, o Promotor pode:
 - comprovar se o número de votos que o SMV entregou está correcto (comparando com o número de autorizações de voto que emitiu),
 - saber o resultado da votação (decifrando os votos com a sua chave privada), e
 - ter a garantia que os votos recebidos deram entrada durante o período da votação.

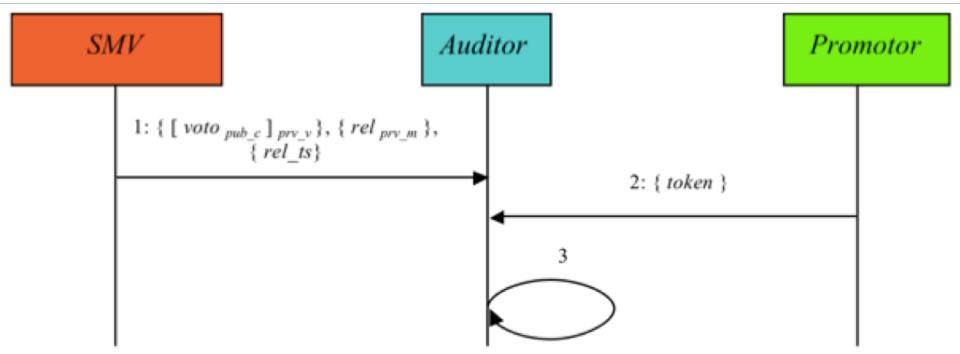
Voto Electrónico – Exemplo 1

- **Auditabilidade**

- Para preservar a confidencialidade do processo de votação, o SMV não pode entregar os votos ao Promotor na sua forma assinada pelo Votante (já que o Promotor passaria a saber quem tinha votado o quê, comprometendo-se o segredo do voto),
- O Promotor pode levantar suspeitas sobre a veracidade e originalidade dos votos entregues pelo SMV;
- Necessária a existência de um **Auditor** que, em caso de dúvida, pode comprovar a idoneidade do SMV utilizando um processo que também não lhe permite saber quem votou o quê.

Voto Electrónico – Exemplo 1

- Auditabilidade – esquema de funcionamento



Passo 1:

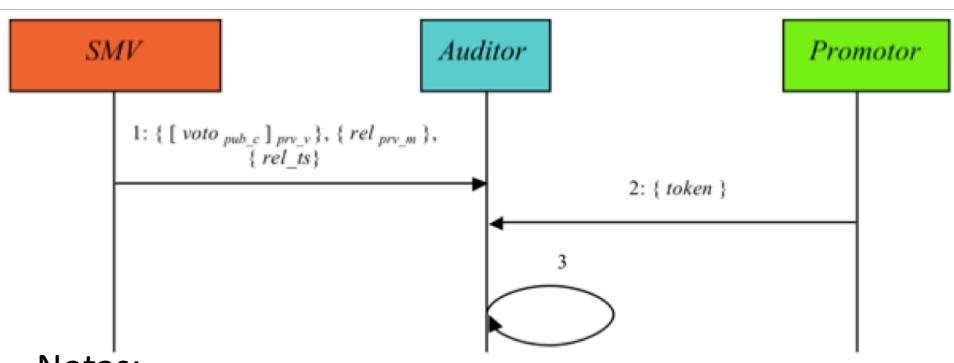
O SMV entrega ao Auditor os votos assinados que recebeu dos Votantes, os relatórios de recepção de votos assinados pelo SMV e os respectivos time-stamps.

Passo 2:

O Promotor entrega ao Auditor a lista dos tokens de autorização que emitiu durante o processo de votação.

Voto Electrónico – Exemplo 1

- Auditabilidade – esquema de funcionamento



Notas:

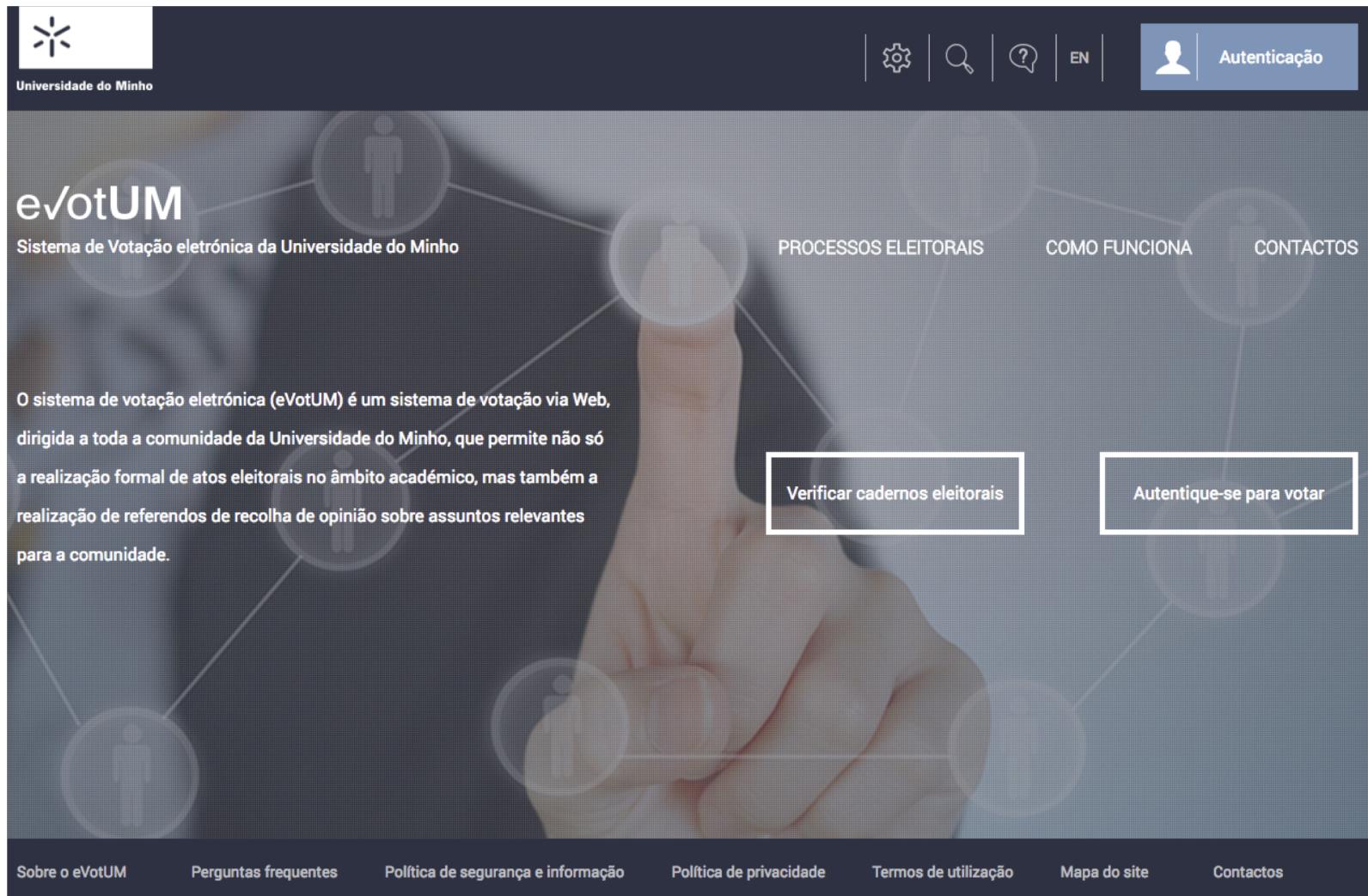
- Os formatos das chaves públicas, certificados, assinaturas digitais, mensagens cifradas e time-stamps utilizados pelo sistema são standard, pelo que o desenvolvimento d(a) aplicação(ões) a utilizar para proceder à auditoria dos dados fornecidos pode ser da responsabilidade do Auditor, garantindo-se deste modo a total independência da auditoria e a transparência de todo o processo de auditoria
- Durante este processo, o Auditor não conseguiu saber mais do que devia, já que o conteúdo dos votos assinados entregues pelo SMV se encontram cifrado para o Promotor, não possuindo o Auditor a chave privada necessária para os abrir.

Passo 3:

- O Auditor verifica se cada voto assinado entregue pelo SMV se encontra assinado com uma chave privada correspondente a uma chave pública contida num dos tokens entregues pelo Promotor.
- Adicionalmente, o Auditor pode verificar se a todos os votos entregues pelo SMV corresponde um relatório de recepção e respectivo time-stamp dentro do período definido para a votação.

Se tal acontecer, estará provado que o SMV não adulterou nenhum dos votos, não tendo por isso o Promotor razões para duvidar do resultado da votação.

Voto Electrónico – Exemplo 2



The screenshot shows the homepage of the eVotUM website. At the top left is the University of Minho logo. The top right features icons for settings, search, help, English version (EN), and authentication. The main title "eVotUM" is displayed prominently, followed by the subtitle "Sistema de Votação eletrónica da Universidade do Minho". Below this, a large image shows a close-up of a person's hand interacting with a digital voting interface. To the left of the image, there is descriptive text about the system. To the right, there are four menu links: "PROCESSOS ELEITORAIS", "COMO FUNCIONA", "CONTACTOS", and two buttons: "Verificar cadernos eleitorais" and "Autentique-se para votar". At the bottom, a footer navigation bar includes links for "Sobre o eVotUM", "Perguntas frequentes", "Política de segurança e informação", "Política de privacidade", "Termos de utilização", "Mapa do site", and "Contactos".

O sistema de votação eletrónica (eVotUM) é um sistema de votação via Web, dirigida a toda a comunidade da Universidade do Minho, que permite não só a realização formal de atos eleitorais no âmbito académico, mas também a realização de referendos de recolha de opinião sobre assuntos relevantes para a comunidade.

[Verificar cadernos eleitorais](#)

[Autentique-se para votar](#)

[Sobre o eVotUM](#) [Perguntas frequentes](#) [Política de segurança e informação](#) [Política de privacidade](#) [Termos de utilização](#) [Mapa do site](#) [Contactos](#)

Voto Electrónico – Exemplo 2

Características



AUTENTICIDADE

Apenas pessoas com direito a voto podem votar.



UNICIDADE

Cada eleitor vota apenas uma vez.



ANONIMATO

Não é possível associar um voto a um eleitor, nem vice-versa.



INTEGRIDADE

Os votos não podem ser modificados ou destruídos.



IRREVELÁVEL

Nenhum eleitor pode provar qual o voto que efetuou.



VERIFICABILIDADE

É possível verificar, de forma independente, que todos os votos foram contados corretamente.

Voto Electrónico – Exemplo 2

Características



AUDITABILIDADE

O sistema de voto eletrónico eVotUM pode ser testado e auditado por entidades independentes.



MOBILIDADE

O sistema de voto eletrónico eVotUM não restringe o local onde se vota.



TRANSPARÊNCIA

O sistema de voto eletrónico eVotUM é claro, exato, preciso e seguro.



DISPONIBILIDADE

O sistema de voto eletrónico eVotUM está sempre disponível durante o período de votação.



DETEÇÃO E RECUPERAÇÃO

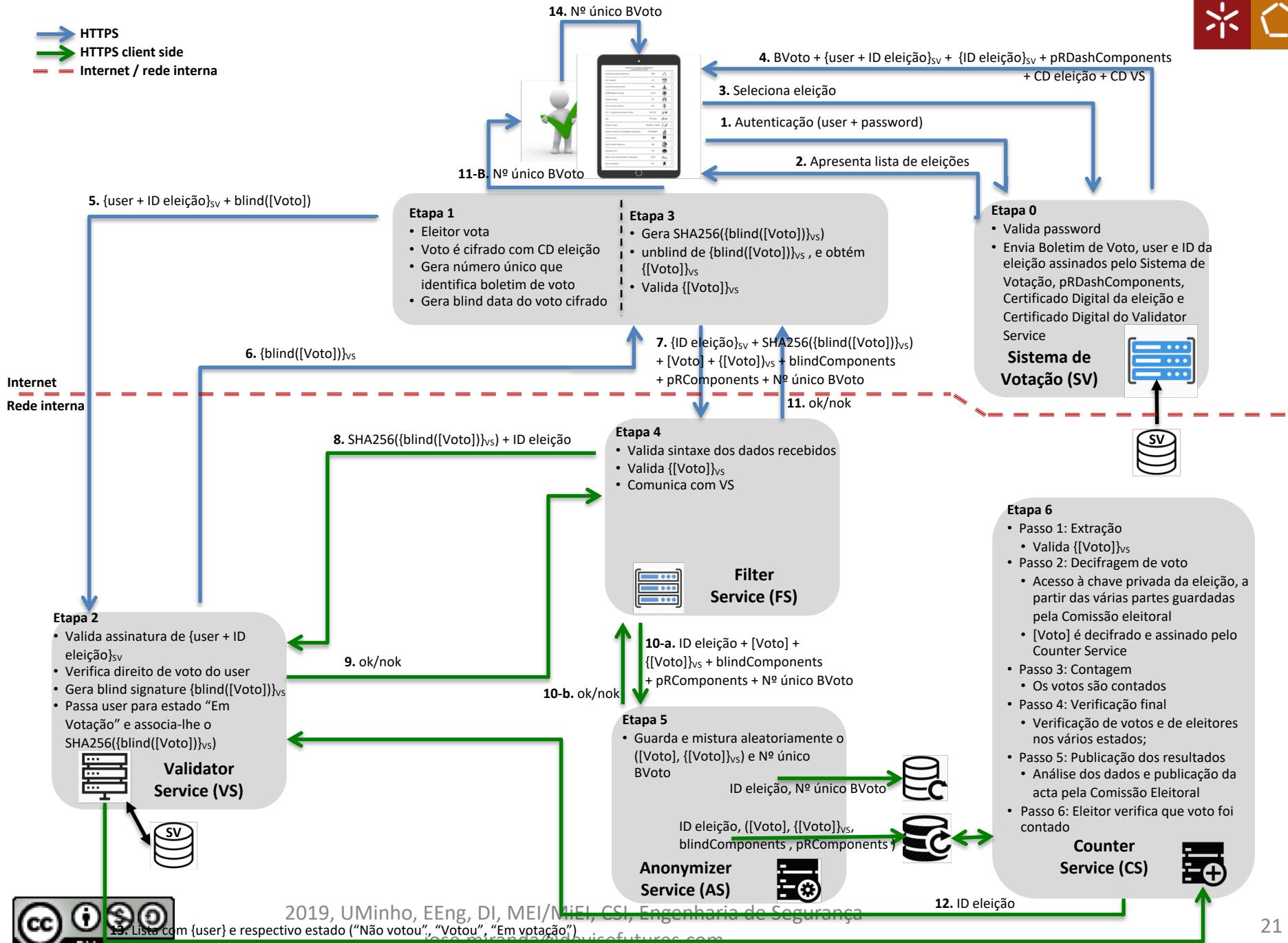
O sistema de voto eletrónico eVotUM deteta erros, falhas e ataques e, recupera a informação até ao ponto de falha.

Voto Electrónico – Exemplo 2

- Etapas e Fluxos de comunicação/mensagens



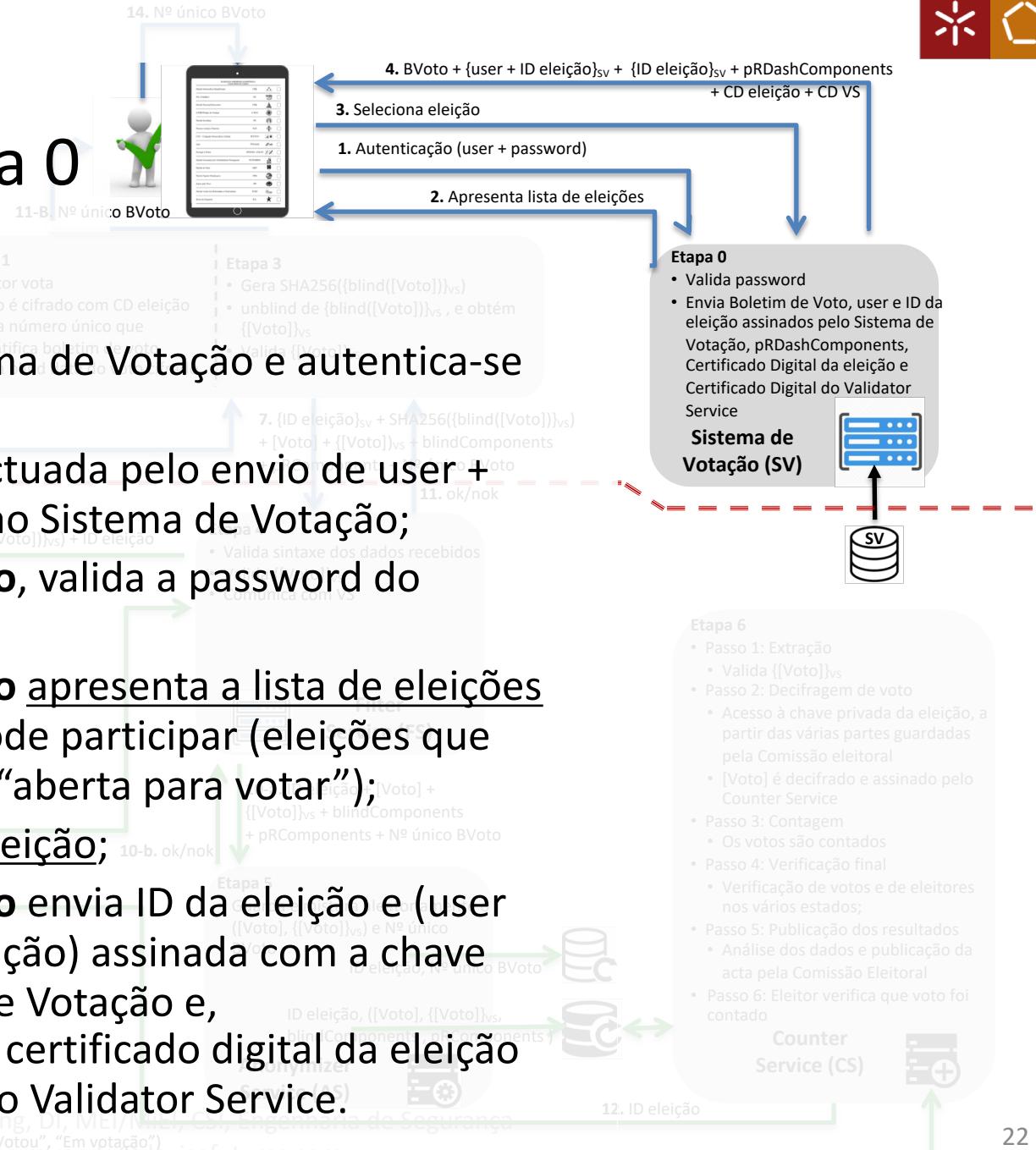
 HTTPS
 HTTPS client side
 Internet / rede interna



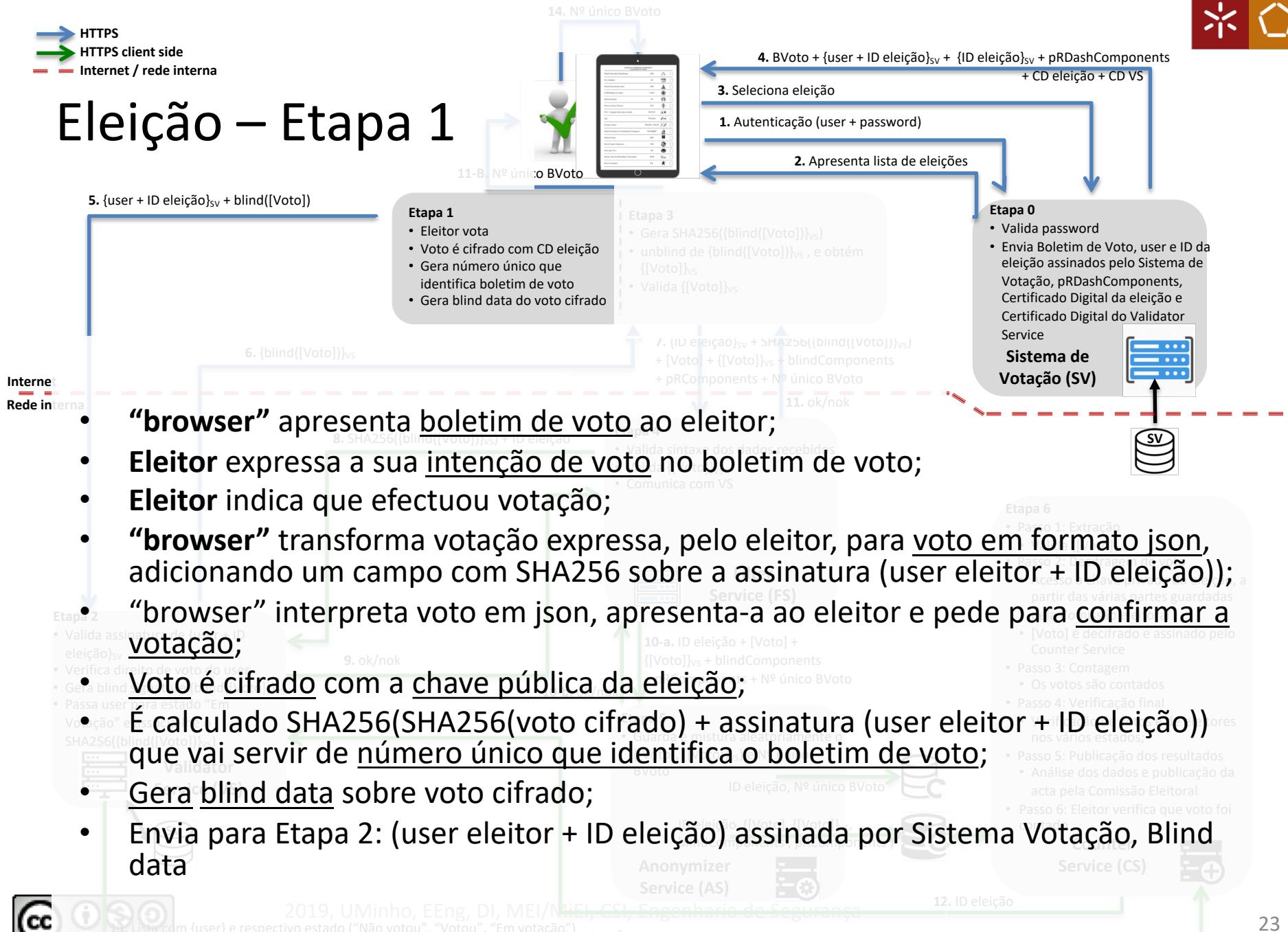
Eleição – Etapa 0

5. $\{\text{user} + \text{ID eleição}\}_{\text{sv}} + \text{blind}([\text{Voto}])$

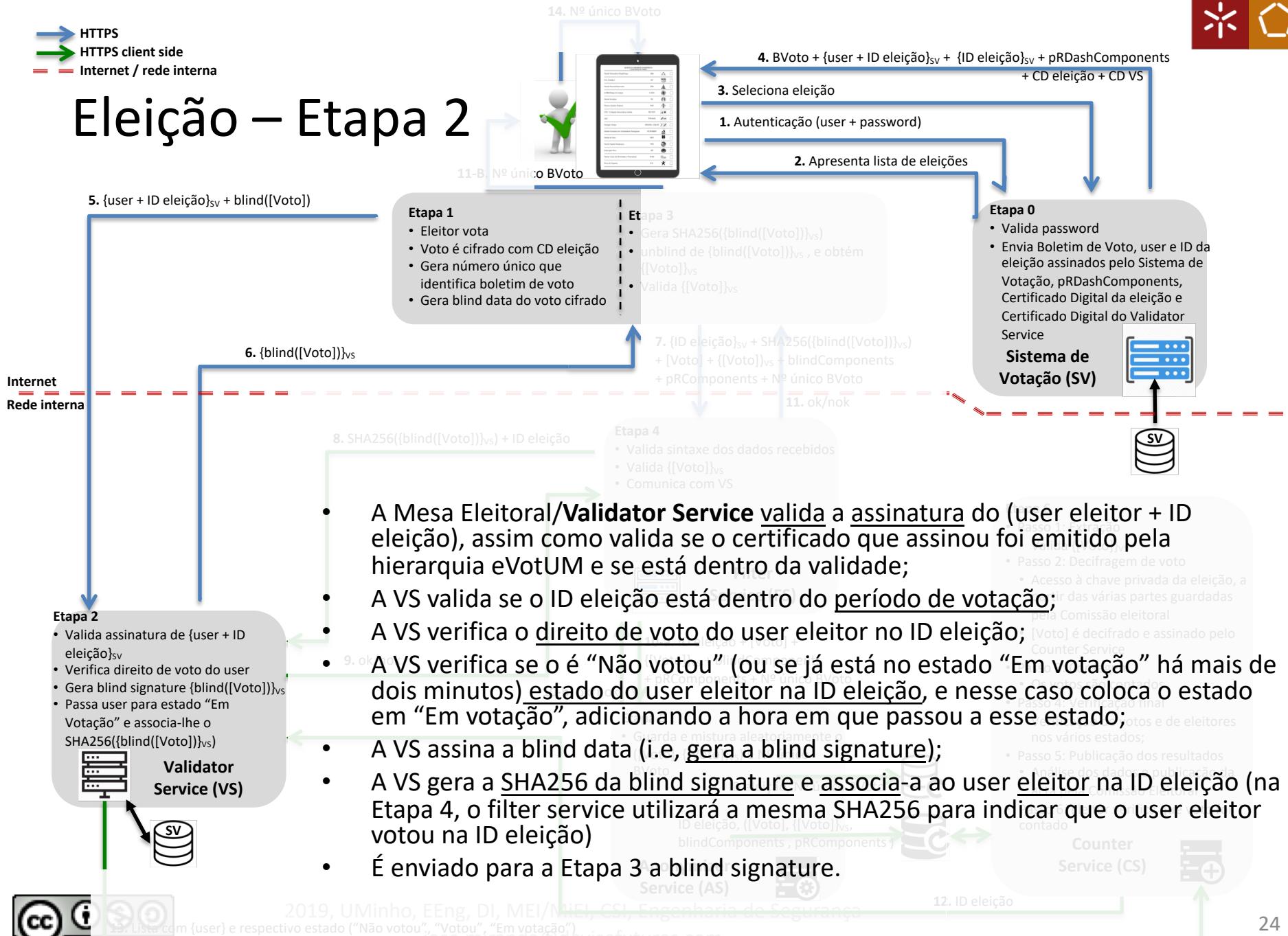
- Eleitor** acede a Sistema de Votação e autentica-se perante o mesmo;
- A autenticação é efectuada pelo envio de **user + password** do eleitor ao Sistema de Votação;
- O **Sistema de Votação**, valida a password do eleitor (PBKDF2);
- O **Sistema de Votação** apresenta a lista de eleições nas quais o eleitor pode participar (eleições que estiverem no estado “aberta para votar”);
- O eleitor seleciona eleição;
- O **Sistema de Votação** envia ID da eleição e (**user** do eleitor + ID da eleição) assinada com a chave privada do Sistema de Votação e, pRDashComponents, certificado digital da eleição e certificado digital do Validator Service.



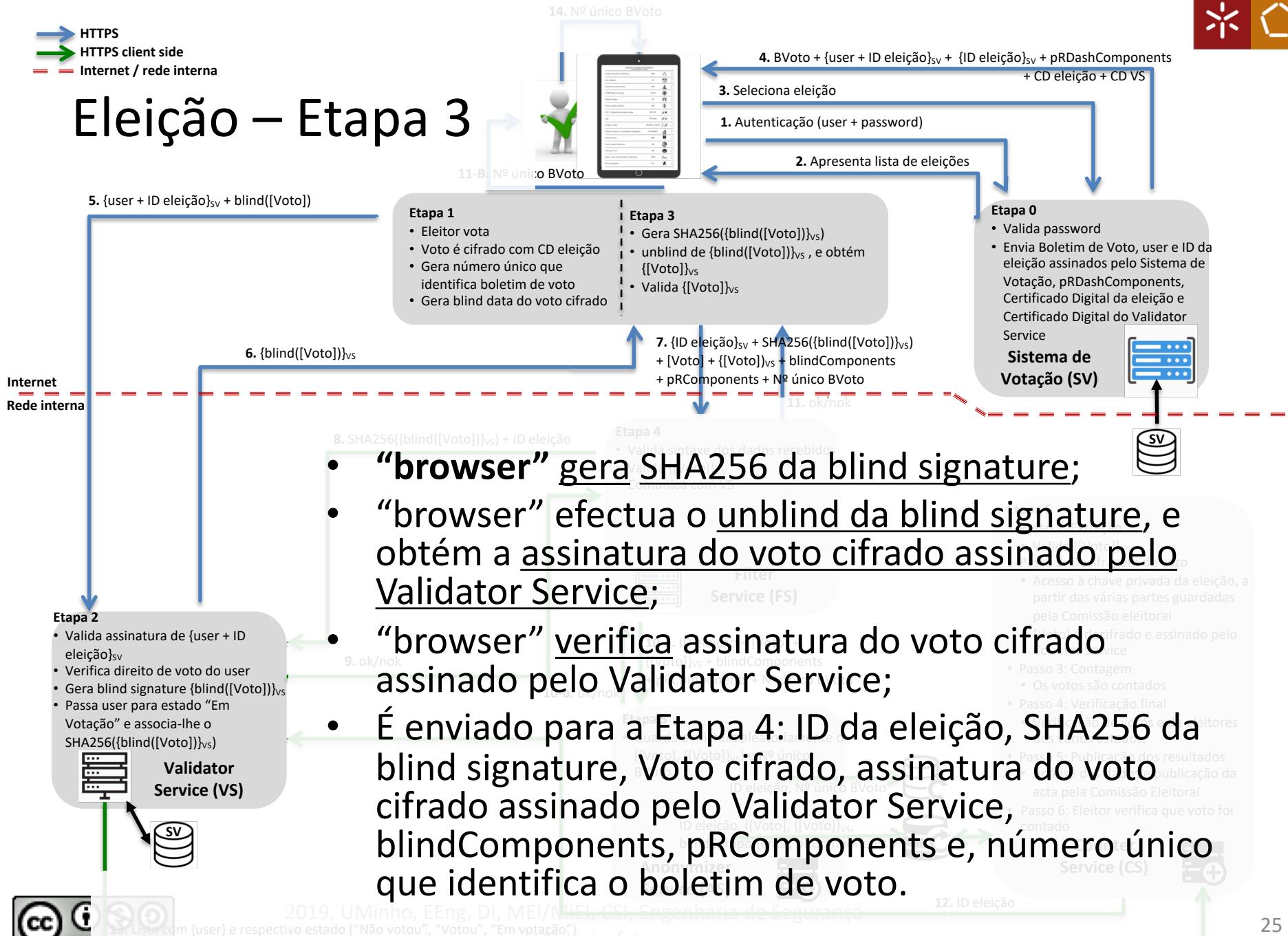
Eleição – Etapa 1

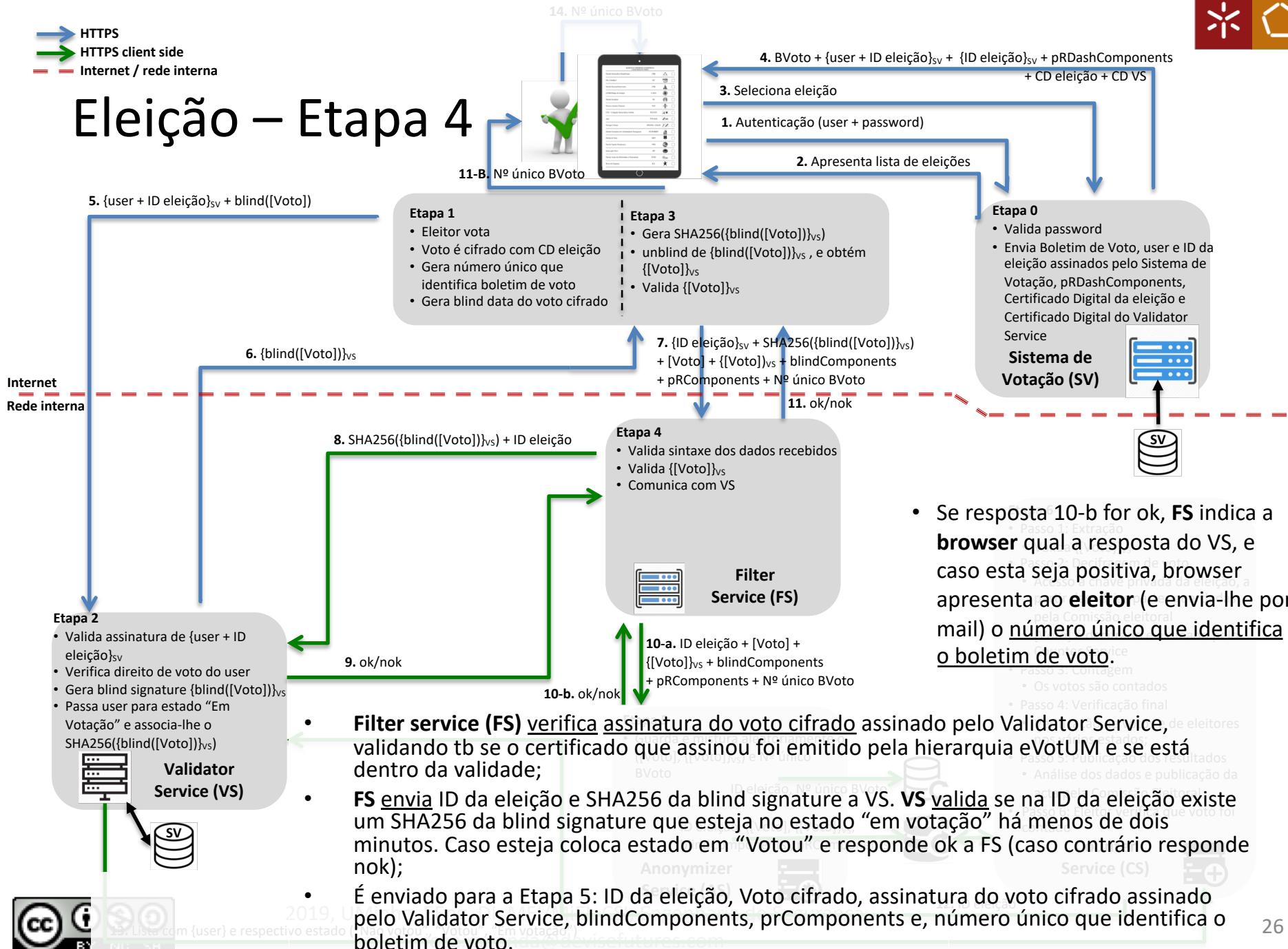


Eleição – Etapa 2



Eleição – Etapa 3







HTTPS
 HTTPS client side
 Internet / rede interna

Eleição – Etapa 5

- O Anonymizer guarda (e mistura aleatoriamente) o Voto cifrado do ID da eleição, a assinatura do voto cifrado assinado pelo Validator Service, blindComponents e pRComponents numa tabela (da Urna eleitoral) e, guarda (e mistura aleatoriamente) o número único que identifica o boletim de voto do ID da eleição noutra tabela (da Urna eleitoral);
- Nota - A mistura aleatória poderá ser efectuada do seguinte modo:
 - Antes do inicio da eleição é criada tabela na Urna eleitoral com o triplo de entradas em relação aos votantes potenciais da eleição;
 - De cada vez que chega um “pacote” para lá colocar é gerado um número aleatório entre 1 e o número de entradas na tabela, que corresponde à linha onde colocar o “pacote”;
 - Se nessa linha já tiver sido colocado um “pacote”, volta-se ao passo anterior, até se encontrar uma linha que não tenha nenhum “pacote”;
 - De referir que são gerados números aleatórios para cada tabela, de modo ao Voto cifrado ser colocados na linha ditado por um número aleatório, e o número único ser colocado na linha ditada por outro número aleatório.

Internet
 Rede interna

Etapa 2

- Valida assinatura de $\{user + ID_{eleição}\}_{sv}$
- Verifica direito de voto do user
- Gera blind signature $\{\text{blind}([Voto])\}_{vs}$
- Passa user para estado “Em Votação” e associa-lhe o $\text{SHA256}(\{\text{blind}([Voto])\}_{vs})$



4. BVoto + {user + ID eleição}_{sv} + {ID eleição}_{sv} + pRDashComponents + CD eleição + CD VS

3. Seleciona eleição

1. Autenticação (user + password)

2. Apresenta lista de eleições

Etapa 0

• Envia Boletim de Voto, user e ID da eleição assinados pelo Sistema de Votação (SV)
• Certificado Digital da Eleição e Certificado Digital do Validator Service

Sistema de

Votação (SV)



10-a. ID eleição + [Voto] + {[Voto]}_{vs} + blindComponents + pRComponents + Nº único BVoto
10-b. ok/nok

Etapa 5

- Guarda e mistura aleatoriamente o $([Voto], {[Voto]}_{vs})$ e Nº único BVoto

ID eleição, Nº único BVoto



ID eleição, $([Voto], {[Voto]}_{vs},$
 $\text{blindComponents, pRComponents})$



Anonymizer
Service (AS)

CSI, Engenharia de Segurança
isfutures.com

12. ID eleição

- [Voto] é decifrado e assinado pelo Counter Service
- Passo 3: Contagem
 - Os votos são contados
- Passo 4: Verificação final
 - Verificação de votos e de eleitores nos vários estados;
- Passo 5: Publicação dos resultados
 - Análise dos dados e publicação da acta pela Comissão Eleitoral
- Passo 6: Eleitor verifica que voto foi contado

Counter
Service (CS)



Eleição – Etapa 6

• Passo 1: Extração

- Counter service verifica assinatura do voto cifrado assinado pelo Validator Service, validando tb se o certificado que assinou foi emitido pela hierarquia eVotUM e se está dentro da validade;

• Passo 2: Decifragem de voto

- É gerada a password de acesso à chave privada da eleição, a partir das várias partes guardadas pela Comissão eleitoral;
- O voto é decifrado, validando-se a estrutura json do voto;
- O voto (com timestamp) é assinado pelo Counter Service, sendo guardado na BD;

• Passo 3: Contagem

- Todos os votos são contados, a partir dos votos assinados;

• Passo 4: Verificação final

- É pedido ao VS o número de eleitores nos vários estados (“Não votou”, “Votou”, “Em votação”) para a eleição;
- É indicado o número de votos recebidos, com assinatura do Validator Service correcta, decifrados correctamente, com a estrutura json do voto decifrado correcta

- **Passo 5: Publicação dos resultados**
- **Passo 6: Eleitor pode verificar se o seu voto foi contado** (através do número único que identifica o boletim de voto).

Internet
Rede interna

