

Mestrado em Engenharia Informática (MEI)

Mestrado Integrado em Engenharia Informática

(MiEI)

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

Engenharia de Segurança



Tópicos

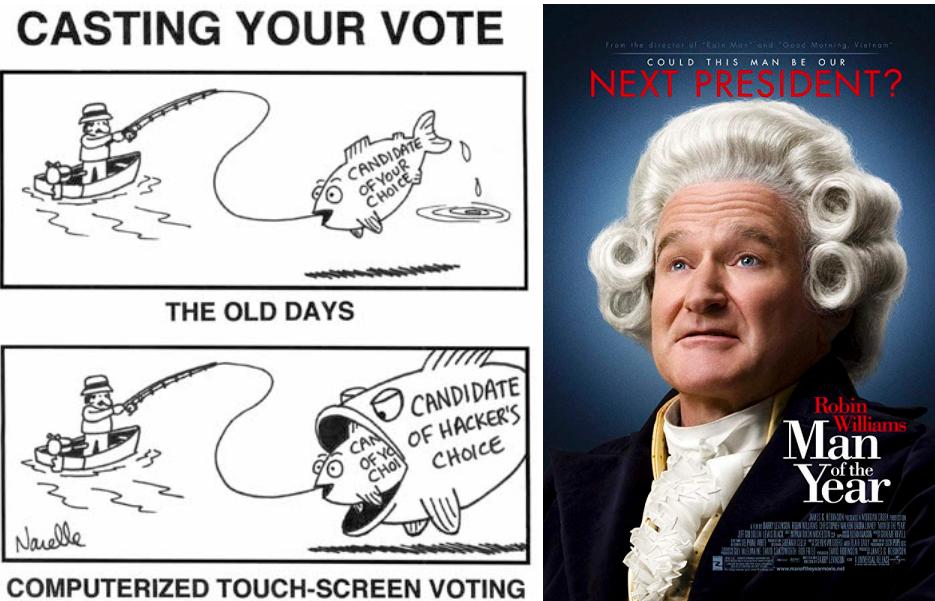
- Criptografia Aplicada
 - Protocolos/aplicações criptográficas
 - Voto eletrónico



Voto Electrónico

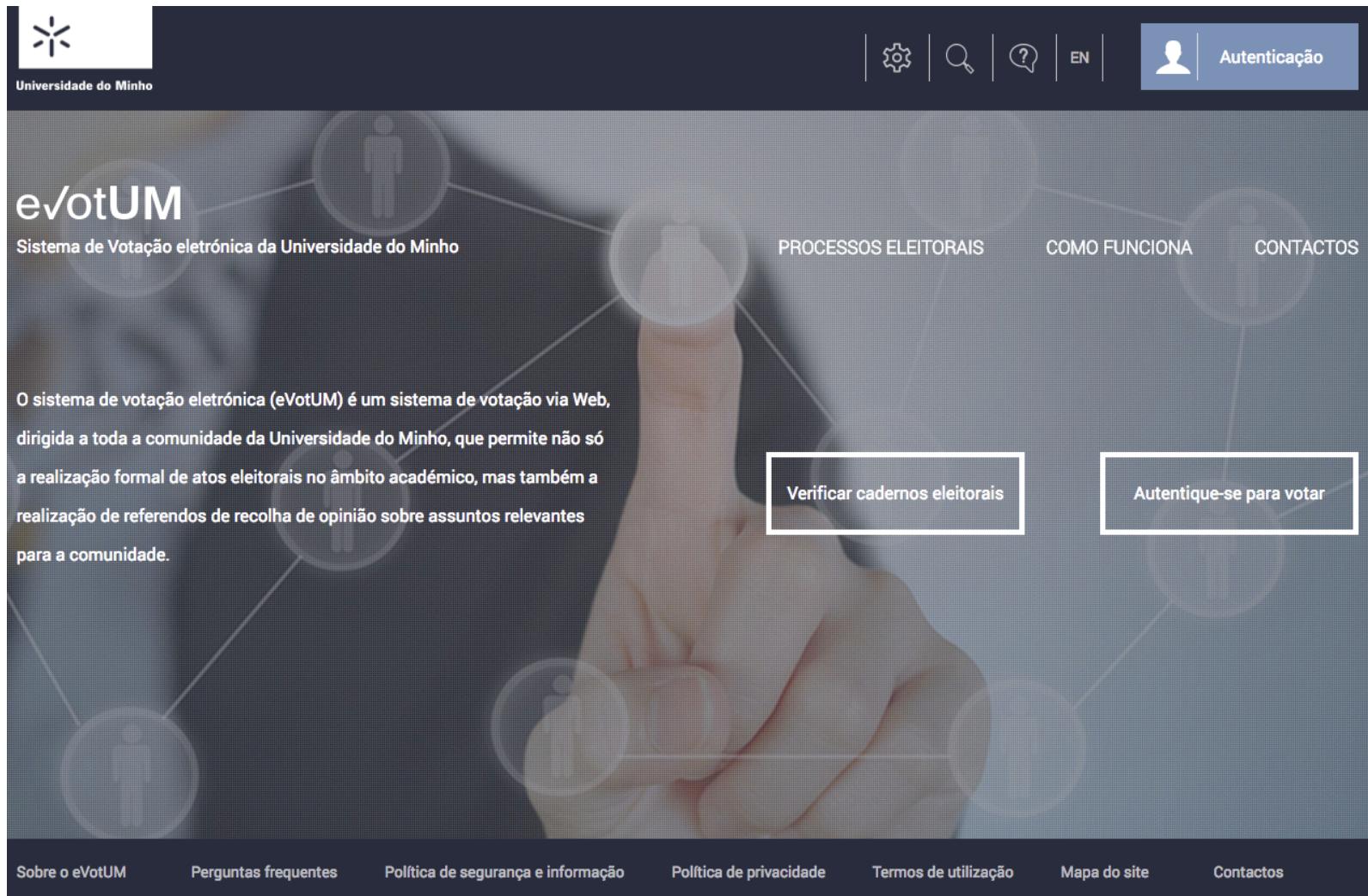
- Protocolo de votação em rede aberta, com as seguintes **garantias gerais**:

- 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 do exemplo apresentado assume que os votantes não dispõem de meios de identificação avançados (como por exemplo, certificado digital pessoal) nem são peritos tecnológicos.

Voto Electrónico – Exemplo



The screenshot shows the homepage of the eVotUM website. At the top left is the University of Minho logo. To the right are icons for settings, search, help, and language (EN). A blue bar on the right contains a user icon and the text "Autenticação". Below the header, the "eVotUM" logo is displayed, followed by the text "Sistema de Votação eletrónica da Universidade do Minho". To the right are three main navigation links: "PROCESSOS ELEITORAIS", "COMO FUNCIONA", and "CONTACTOS". On the left, there is a descriptive text block about the system, and on the right, two buttons: "Verificar cadernos eleitorais" and "Autentique-se para votar". The footer contains 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](#)

Voto Electrónico – Exemplo

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

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

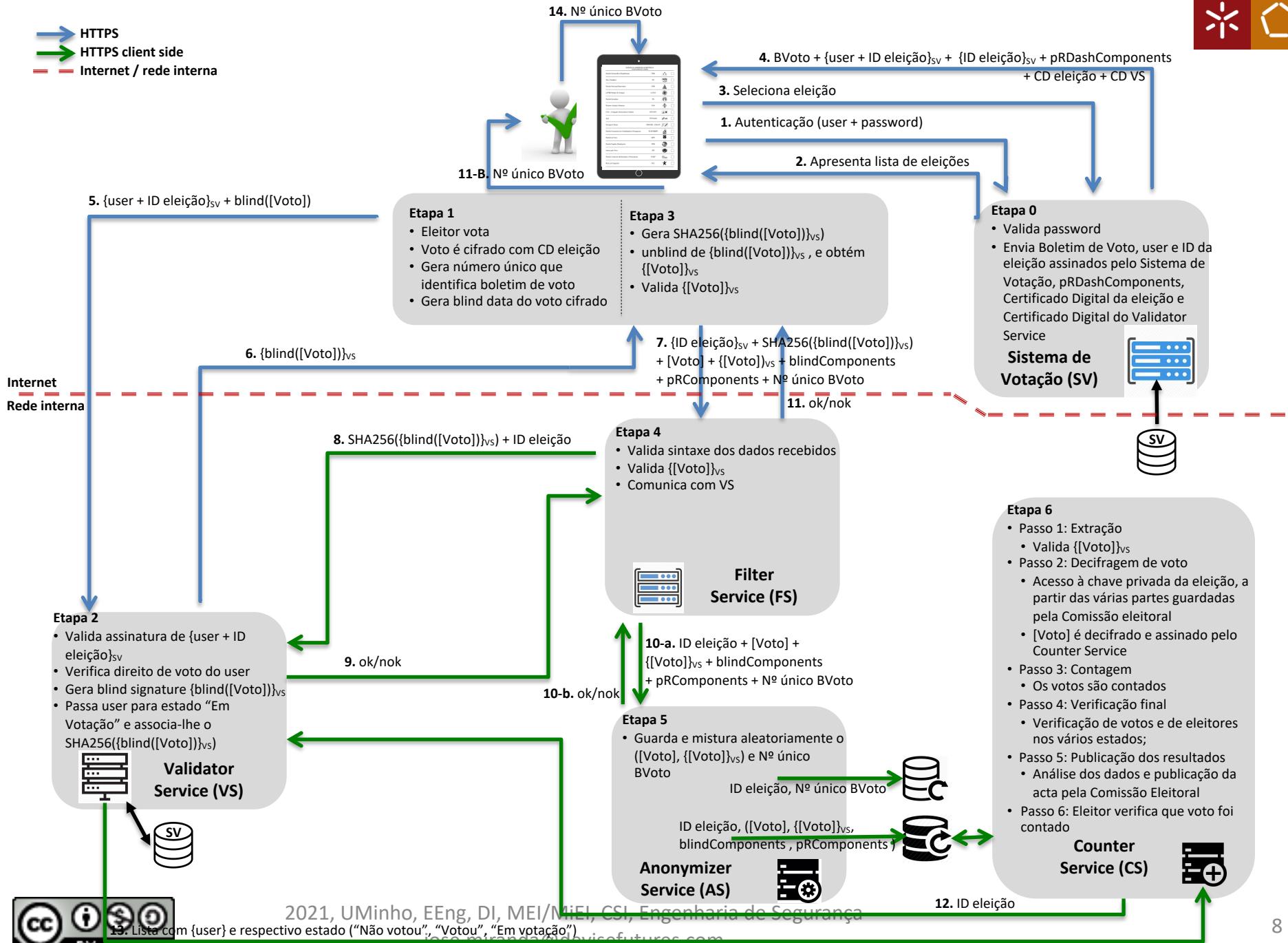
O sistema de voto eletrónico eVotUM deteta erros, falhas e ataques e, recupera a informação até ao ponto de falha.

Voto Electrónico – Exemplo

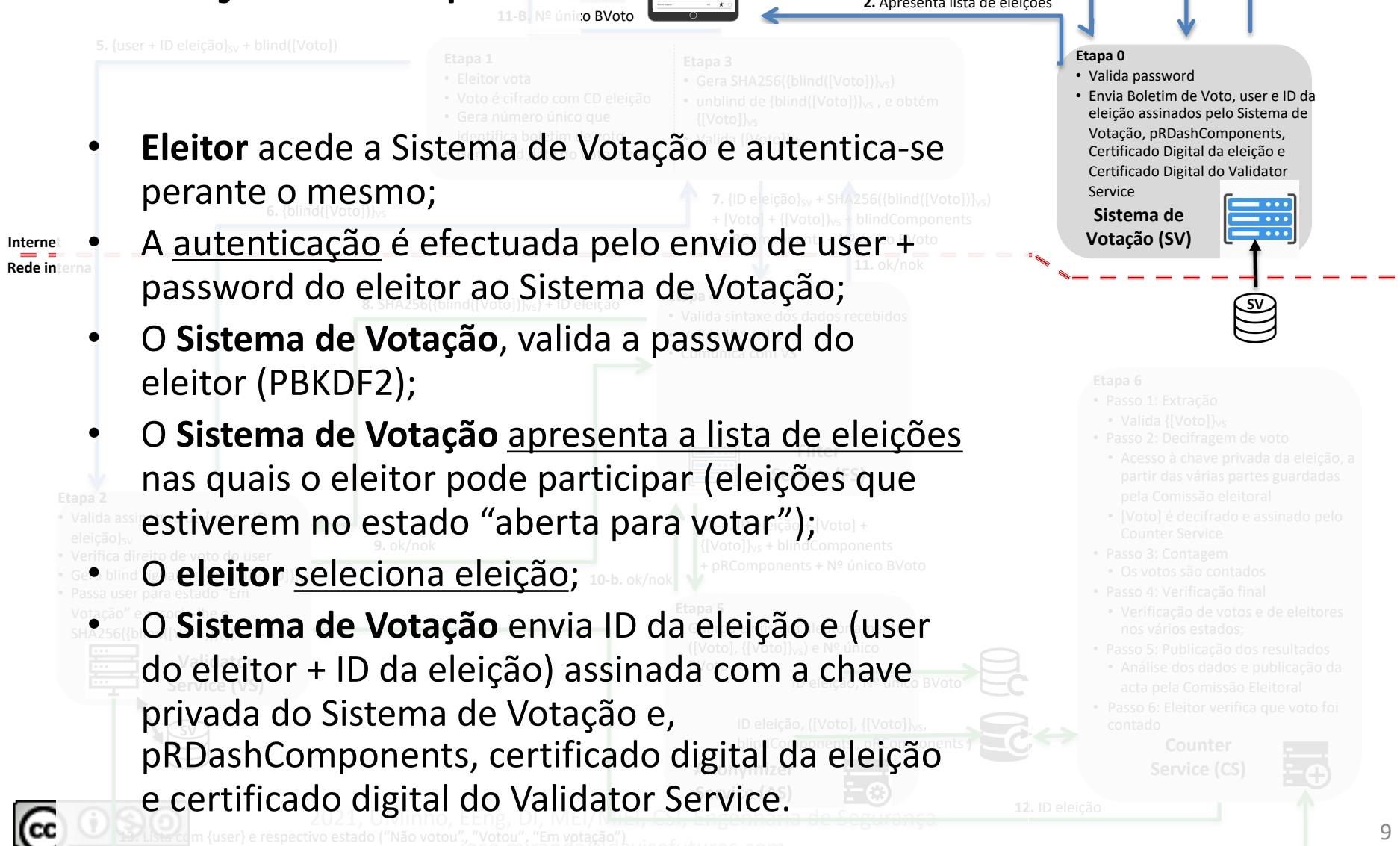
- Etapas e Fluxos de comunicação/mensagens



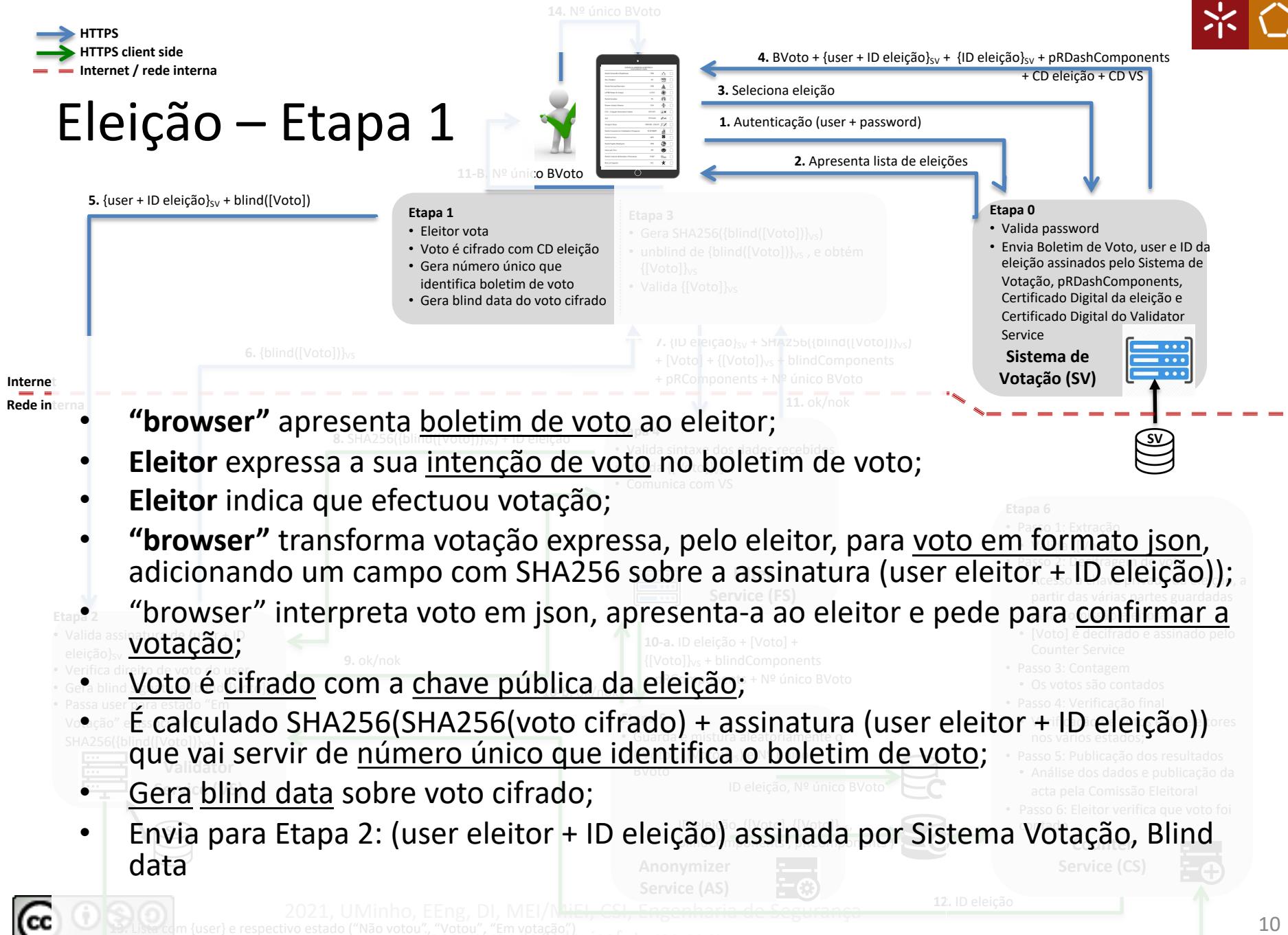
 HTTPS
 HTTPS client side
 Internet / rede interna



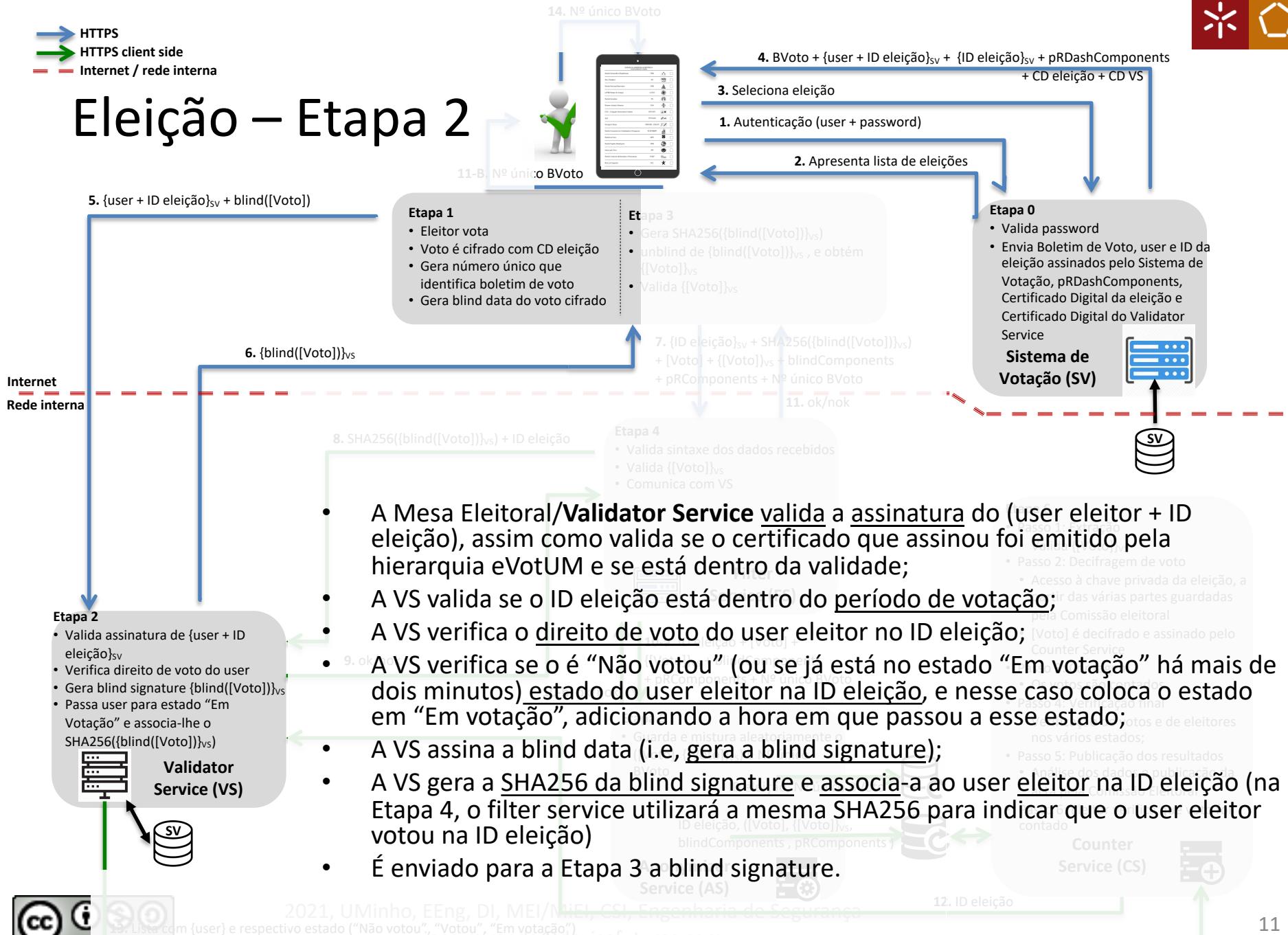
Eleição – Etapa 0



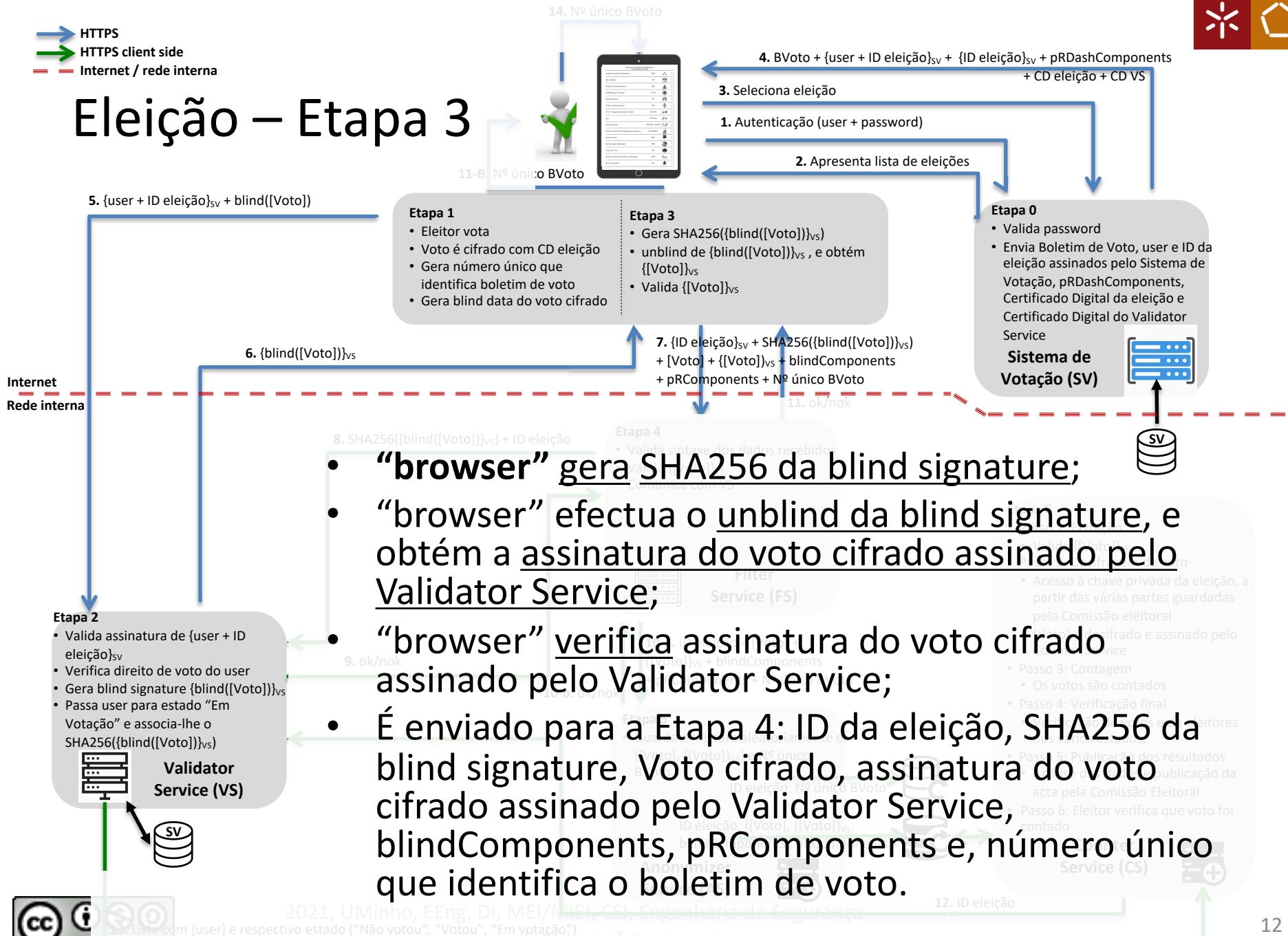
Eleição – Etapa 1

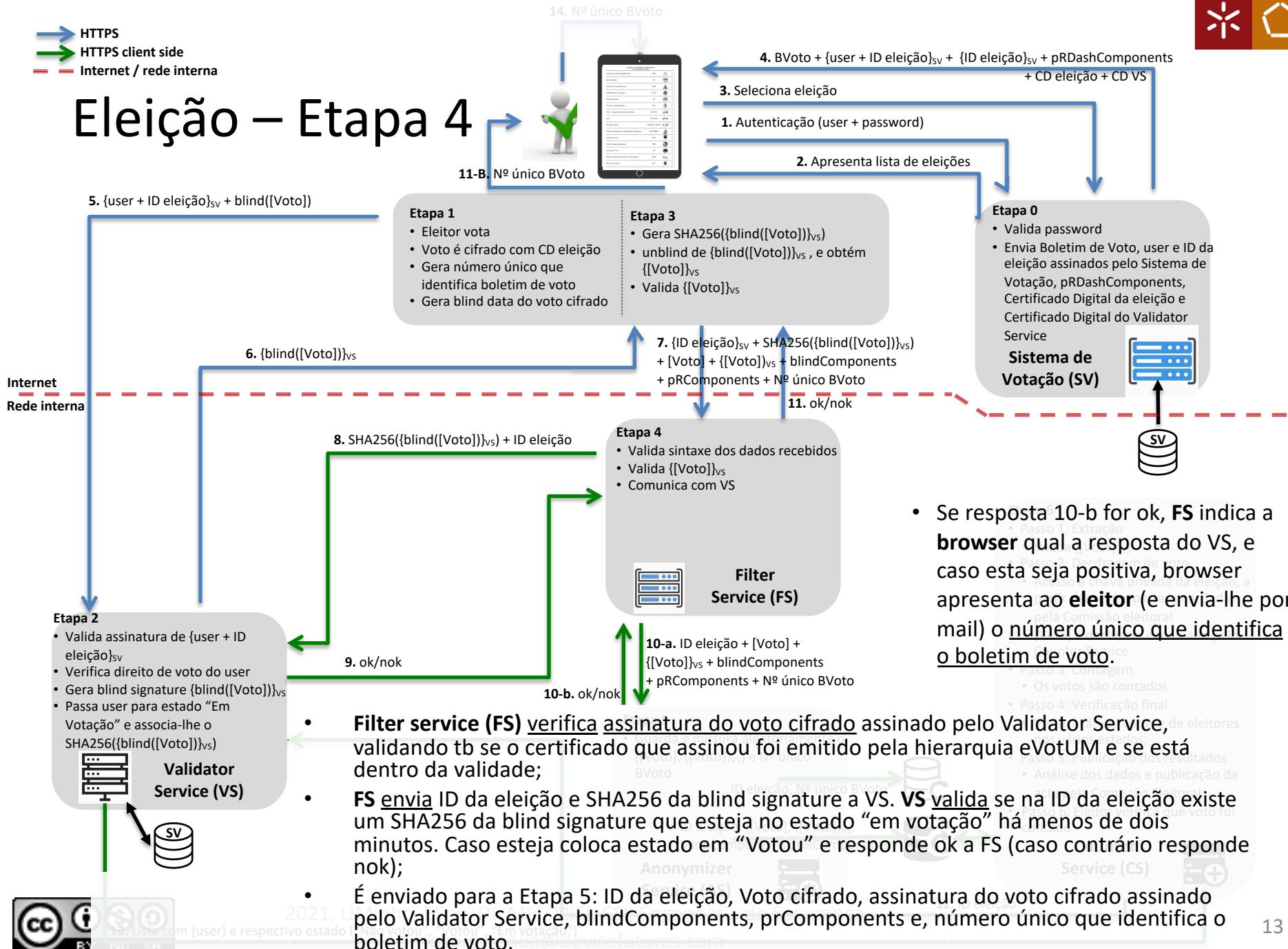


Eleição – Etapa 2



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 $\text{SHA256}(\{\text{blind}([Voto])\}_{vs})$



14. Nº único BVoto

11-B. Nº único BVoto

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 4

• 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)

• Sist

ema de

Votação

(SV)

12. ID eleição

13. Lista com {user} e respectivo resultado ("BVoto")

14. Nº único BVoto

15. ID eleição

16. ID eleição

17. ID eleição

18. ID eleição

19. ID eleição

20. ID eleição

21. ID eleição

22. ID eleição

23. ID eleição

24. ID eleição

25. ID eleição

26. ID eleição

27. ID eleição

28. ID eleição

29. ID eleição

30. ID eleição

31. ID eleição

32. ID eleição

33. ID eleição

34. ID eleição

35. ID eleição

36. ID eleição

37. ID eleição

38. ID eleição

39. ID eleição

40. ID eleição

41. ID eleição

42. ID eleição

43. ID eleição

44. ID eleição

45. ID eleição

46. ID eleição

47. ID eleição

48. ID eleição

49. ID eleição

50. ID eleição

51. ID eleição

52. ID eleição

53. ID eleição

54. ID eleição

55. ID eleição

56. ID eleição

57. ID eleição

58. ID eleição

59. ID eleição

60. ID eleição

61. ID eleição

62. ID eleição

63. ID eleição

64. ID eleição

65. ID eleição

66. ID eleição

67. ID eleição

68. ID eleição

69. ID eleição

70. ID eleição

71. ID eleição

72. ID eleição

73. ID eleição

74. ID eleição

75. ID eleição

76. ID eleição

77. ID eleição

78. ID eleição

79. ID eleição

80. ID eleição

81. ID eleição

82. ID eleição

83. ID eleição

84. ID eleição

85. ID eleição

86. ID eleição

87. ID eleição

88. ID eleição

89. ID eleição

90. ID eleição

91. ID eleição

92. ID eleição

93. ID eleição

94. ID eleição

95. ID eleição

96. ID eleição

97. ID eleição

98. ID eleição

99. ID eleição

100. ID eleição

101. ID eleição

102. ID eleição

103. ID eleição

104. ID eleição

105. ID eleição

106. ID eleição

107. ID eleição

108. ID eleição

109. ID eleição

110. ID eleição

111. ID eleição

112. ID eleição

113. ID eleição

114. ID eleição

115. ID eleição

116. ID eleição

117. ID eleição

118. ID eleição

119. ID eleição

120. ID eleição

121. ID eleição

122. ID eleição

123. ID eleição

124. ID eleição

125. ID eleição

126. ID eleição

127. ID eleição

128. ID eleição

129. ID eleição

130. ID eleição

131. ID eleição

132. ID eleição

133. ID eleição

134. ID eleição

135. ID eleição

136. ID eleição

137. ID eleição

138. ID eleição

139. ID eleição

140. ID eleição

141. ID eleição

142. ID eleição

143. ID eleição

144. ID eleição

145. ID eleição

146. ID eleição

147. ID eleição

148. ID eleição

149. ID eleição

150. ID eleição

151. ID eleição

152. ID eleição

153. ID eleição

154. ID eleição

155. ID eleição

156. ID eleição

157. ID eleição

158. ID eleição

159. ID eleição

160. ID eleição

161. ID eleição

162. ID eleição

163. ID eleição

164. ID eleição

165. ID eleição

166. ID eleição

167. ID eleição

168. ID eleição

169. ID eleição

170. ID eleição

171. ID eleição

172. ID eleição

173. ID eleição

174. ID eleição

175. ID eleição

176. ID eleição

177. ID eleição

178. ID eleição

179. ID eleição

180. ID eleição

181. ID eleição

182. ID eleição

183. ID eleição

184. ID eleição

185. ID eleição

186. ID eleição

187. ID eleição

188. ID eleição

189. ID eleição

190. ID eleição

191. ID eleição

192. ID eleição

193. ID eleição

194. ID eleição

195. ID eleição

196. ID eleição

197. ID eleição

198. ID eleição

199. ID eleição

200. ID eleição

201. ID eleição

202. ID eleição

203. ID eleição

204. ID eleição

205. ID eleição

206. ID eleição

207. ID eleição

208. ID eleição

209. ID eleição

210. ID eleição

211. ID eleição

212. ID eleição

213. ID eleição

214. ID eleição

215. ID eleição

216. ID eleição

217. ID eleição

218. ID eleição

219. ID eleição

220. ID eleição

221. ID eleição

222. ID eleição

223. ID eleição

224. ID eleição

225. ID eleição

226. ID eleição

227. ID eleição

228. ID eleição

229. ID eleição

230. ID eleição

231. ID eleição

232. ID eleição

233. ID eleição

234. ID eleição

235. ID eleição

236. ID eleição

237. ID eleição

238. ID eleição

239. ID eleição

240. ID eleição

241. ID eleição

242. ID eleição

243. ID eleição

244. ID eleição

245. ID eleição

246. ID eleição

247. ID eleição

248. ID eleição

249. ID eleição

250. ID eleição

251. ID eleição

252. ID eleição

253. ID eleição

254. ID eleição

255. ID eleição

256. ID eleição

257. ID eleição

258. ID eleição

259. ID eleição

260. ID eleição

261. ID eleição

262. ID eleição

263. ID eleição

264. ID eleição

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).