

QR Code no Boletim de Urna

Manual para
a criação de
aplicativos
de leitura



Brasília
TSE
2024

© 2024 Tribunal Superior Eleitoral

É permitida a reprodução parcial desta obra desde que citada a fonte.

Secretaria de Gestão da Informação e do Conhecimento

SAFS, Quadra 7, Lotes 1/2, 1º andar

Brasília/DF – 70095-901

Telefone: (61) 3030-9225

Secretária-Geral da Presidência

Andrea Maciel Pachá

Diretora-Geral da Secretaria do Tribunal

Roberta Maia Gresta

Secretário de Gestão da Informação e do Conhecimento

Cleber Schumann

Coordenador de Editoração e Publicações

Washington Luiz de Oliveira

Conteúdo

Seção de Voto Informatizado

Capa e projeto gráfico

Wagner Castro e Pedro Henrique Silva

Seção de Editoração e Programação Visual (Seprov/Cedip/SGIC)

Diagramação

Wagner de Castro

Seção de Editoração e Programação Visual (Seprov/Cedip/SGIC)

Revisão editorial

Harrison da Rocha e Patrícia Jacob

Seção de Preparação e Revisão de Conteúdos (Seprev/Cedip/SGIC)

TRIBUNAL SUPERIOR ELEITORAL

Presidente

Ministra Cármen Lúcia

Vice-Presidente

Ministro Nunes Marques

Ministros

Ministro André Mendonça

Ministro Raul Araújo

Ministra Isabel Gallotti

Ministro Floriano de Azevedo Marques

Ministro Ramos Tavares

Procurador-Geral Eleitoral

Paulo Gonet Branco

QR Code no Boletim de Urna

Manual para a criação de
aplicativos de leitura

Sumário

1. APRESENTAÇÃO	6
2. O BOLETIM DE URNA (BU)	7
3. POR QUE QR CODE E COMO ELE FOI IMPLANTADO	14
4. FORMATO DE REPRESENTAÇÃO DO BOLETIM DE URNA (BU)	14
4.1. CABEÇALHO	15
4.2. CONTEÚDO DO BOLETIM	15
4.3. SEGURANÇA	18
5. CÓDIGO DOS CARGOS	18
5.1. EXEMPLOS	18
6. ASSINATURA DIGITAL	20
6.1. FORMAÇÃO DA ASSINATURA	21
6.2. INSTRUÇÕES PARA A VERIFICAÇÃO DE ASSINATURA DIGITAL E EXEMPLOS DE CÓDIGO	21
7. COMPLEMENTO DOS DADOS – NOMES DAS CANDIDATAS, DOS CANDIDATOS, DOS CARGOS E DAS ELEIÇÕES	25
7.1. SCHEMA JSON	25
7.2. VERIFICAÇÃO DE ASSINATURA DO ARQUIVO DE COMPLEMENTO DOS DADOS	38
8. GLOSSÁRIO	40



1. APRESENTAÇÃO

A Justiça Eleitoral está em constante mudança para a adoção do que há de mais moderno no que se refere a eleições, tudo com o objetivo de promover um processo transparente, seguro e eficiente. Desde a implantação da urna eletrônica, há quase 28 anos, esta Justiça Especializada aperfeiçoa seus sistemas e equipamentos todos os anos, adicionando novos mecanismos que promovam a fiscalização cidadã e garantam a segurança do sistema eleitoral brasileiro.

As formas mais antigas de fiscalização são a impressão e a publicação do Boletim de Urna (BU). Encerrada a votação, a urna apura os votos e emite um relatório com o resultado oficial da seção eleitoral. Esse relatório é um documento público, cuja cópia é afixada no local de votação para que qualquer cidadã ou cidadão possa conferir.

Além disso, cópias do boletim são garantidas às(aos) fiscais partidárias(os), podendo, ainda, ser entregues a interessadas e a interessados presentes no momento do fechamento da votação. A partir dos BUs, os partidos políticos já podem iniciar uma totalização própria para comparar com a realizada pela Justiça Eleitoral. Nos dias que se seguem, o boletim impresso pode ser conferido na internet com o resultado processado pelos sistemas eleitorais.

Esse é um mecanismo de acompanhamento simples, já presente nos sistemas há alguns anos. Com a impressão, a publicação e a conferência do boletim na internet, os órgãos eleitorais mitigam quaisquer suspeitas que possam existir sobre o transporte e a totalização dos resultados das seções.

Entretanto, com o crescente interesse das pessoas no acompanhamento do processo eleitoral, faz-se necessário o aprimoramento dos meios de fiscalização já disponibilizados. Nesse sentido, a partir das Eleições 2016, o BU passou a contar com um QR Code, que permite a rápida digitalização do resultado apurado numa seção. A tecnologia QR Code – *Quick Response Code* (código de resposta rápida) – é um tipo de código de barras em duas dimensões, capaz de armazenar muito mais informação que um código de barras comum¹. Dessa forma, um número muito maior de pessoas poderá obter cópias dos resultados apurados pelas urnas, mais seções terão os seus resultados validados e a conferência da totalização será mais rápida e fácil.

Diante disso, a Justiça Eleitoral desenvolveu um aplicativo para dispositivos móveis que permite a digitalização e a conferência do BU. Mas, com o intuito de que esse instrumento seja uma forma ainda mais eficaz de fiscalização cidadã, esta Justiça está fornecendo todas as instruções necessárias para que qualquer pessoa interessada desenvolva um aplicativo próprio de leitura do boletim, provendo também os meios necessários para a validação da sua integridade e autenticidade.

Este documento apresenta a terminologia utilizada pela Justiça Eleitoral, descreve a tecnologia adotada, o formato de representação digital do BU no QR Code, os mecanismos de assinatura digital e o modo de obtenção dos dados complementares para a correta reconstrução do boletim impresso.

Dúvidas, críticas ou sugestões podem ser encaminhadas ao endereço qrcodenobu@tse.jus.br.

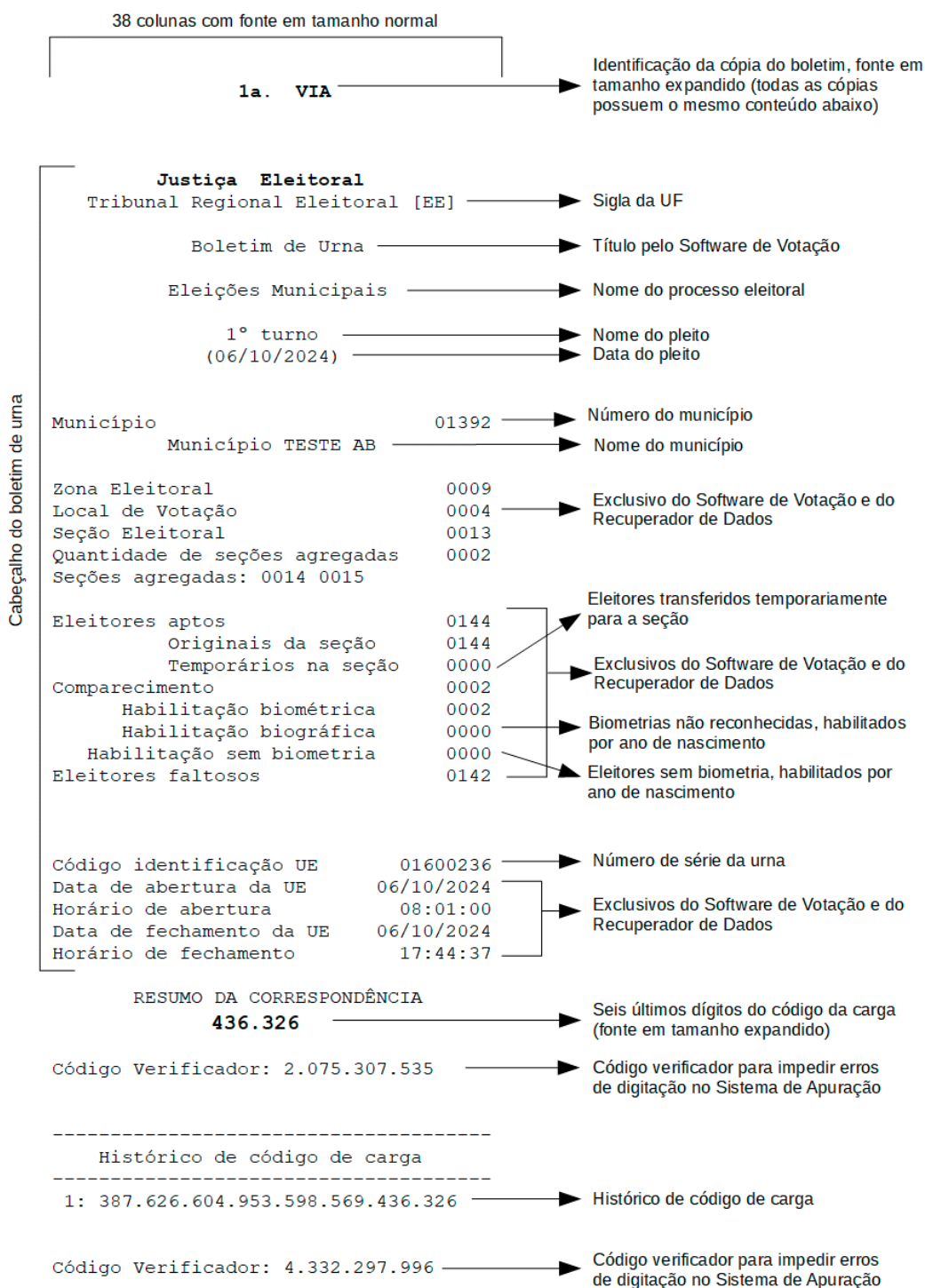
Democracia se faz com colaboração. Participe.

¹ Disponível em: <https://en.wikipedia.org/wiki/QR_code>.



2. O BOLETIM DE URNA (BU)

A seguir, será apresentada uma visão detalhada do BU impresso pelo Software de Votação (VOTA), suas seções e todos os dados presentes.





=====SIMULADO=====

-----VEREADOR-----

Partido: 93 - PProf

Nome do candidato Num cand Votos

Professora 93001 0001

Votos de legenda 0000

Total do partido 0001

Código Verificador: 9.535.327.739

Nome do cargo

Número e sigla do partido; marca o início dos votos para o partido e seus candidatos (apenas para cargos proporcionais)

Código verificador para impedir erros de digitação no Sistema de Apuração

Eleitores aptos 0144

 Originais da seção 0144

 Temporários na seção 0000

Total de votos nominais 0001

Total de votos de legenda 0000

Branco 0001

Nulos 0000

Total apurado 0002

Contadores de eleitores aptos temporários para o cargo

Código Verificador: 0.458.882.182

Código verificador para impedir erros de digitação no Sistema de Apuração

=====SIMULADO=====

-----PREFEITO-----

Nome do candidato Num cand Votos

Forró 92 0001

Eleitores Aptos 0144

 Originais da seção 0144

 Temporários na seção 0000

Total de votos Nominais 0001


Branco 0000

Nulos 0001

Total Apurado 0002

Código Verificador: 2.004.042.513

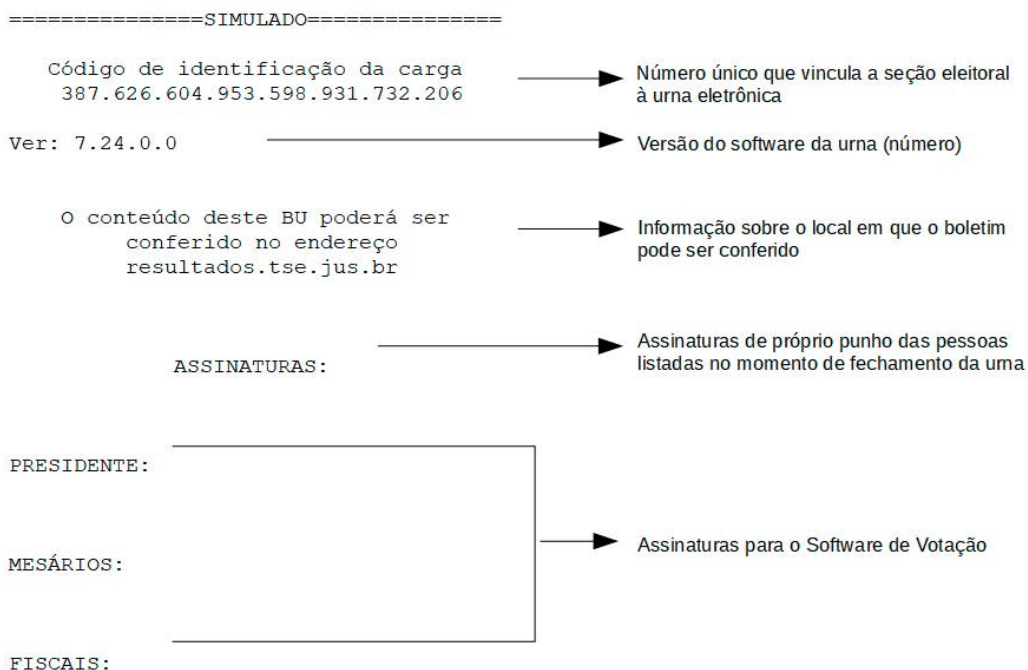
Código verificador para impedir erros de digitação no Sistema de Apuração



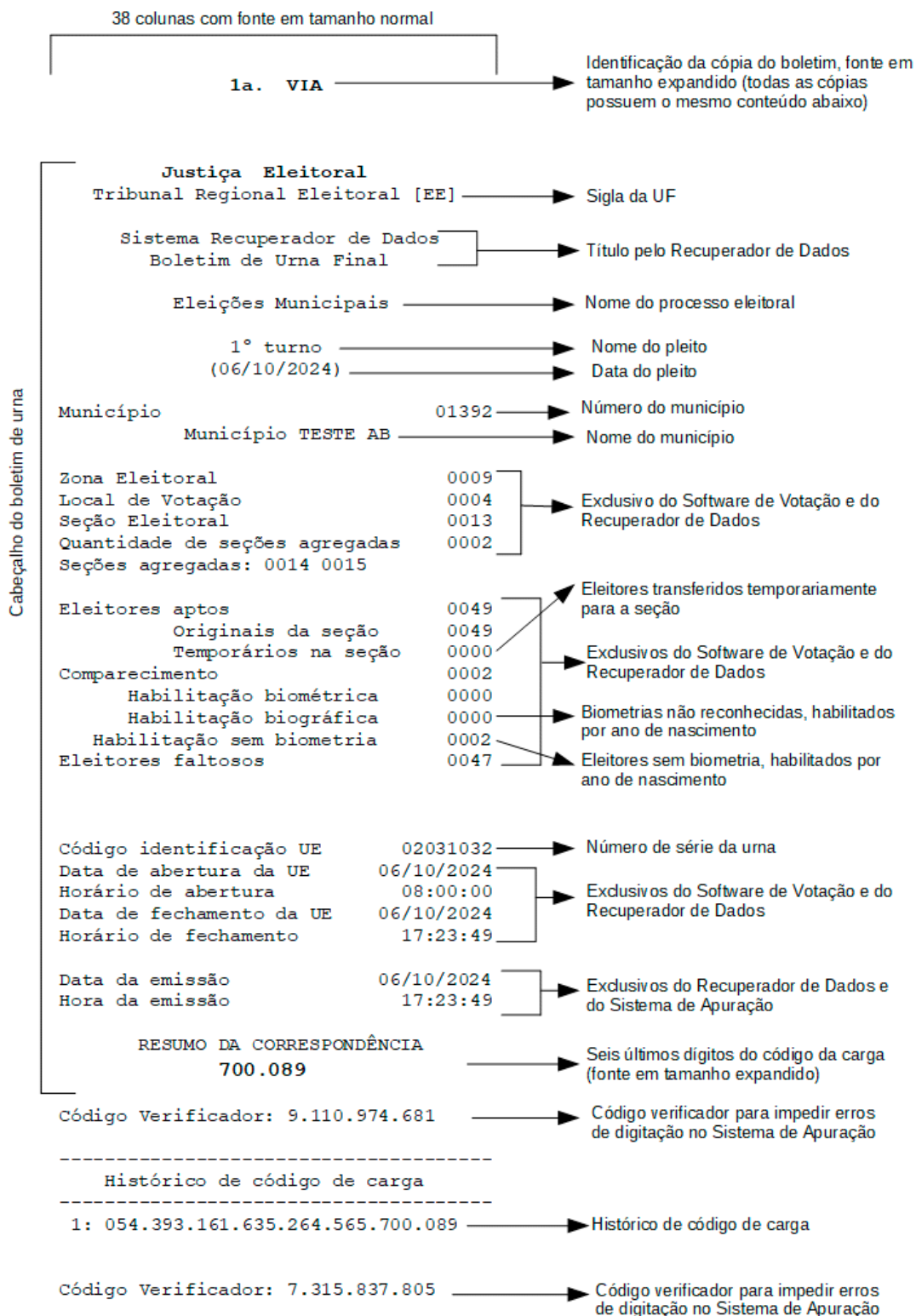
QR Code impresso

ASSINATURA QR CODE:
B2FA068D49111BA3A61DA0DC44334F8EC41598
C73DE90B8E22AA64DAB8C10AA083FD0737B475
60B3C6C837D0F24044ABB18DD5A4D2BC66884D
B57BFCFA40F906

Assinatura do conteúdo do QR Code (igual ao codificado dentro do QR Code)

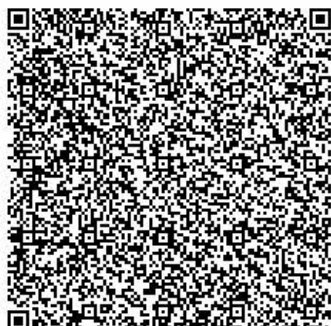


A seguir, uma visão do cabeçalho do BU impresso pelo Recuperador de Dados e seu respectivo QR Code. O corpo do boletim foi omitido devido a sua semelhança com o Boletim do Software de Votação.





=====



QR Code impresso

ASSINATURA QR CODE:
DBCC7BFDA45F0F9D06FC1EF825DD699EFB9487
C05ABC3CD482978B259CE18878486214D77110
1DC97AD554C8CD80E7577A743042EDBB83C0AB
8CFF96FEF7650D



Assinatura do conteúdo do QR Code (igual
ao codificado dentro do QR Code)

=====SIMULADO=====

Código de identificação da carga
054.393.161.635.264.565.700.089



Número único que vincula a seção eleitoral
à urna eletrônica

Ver: 9.20.0.0



Versão do software da urna (número)

o conteúdo deste BU poderá ser
conferido no endereço
resultados.tse.jus.br



Local onde o boletim será disponibilizado
para conferência

ASSINATURAS:



Assinaturas de próprio punho das pessoas
listadas no momento de fechamento da urna

PRESIDENTE DA JUNTA:

COMPONENTES DA JUNTA:

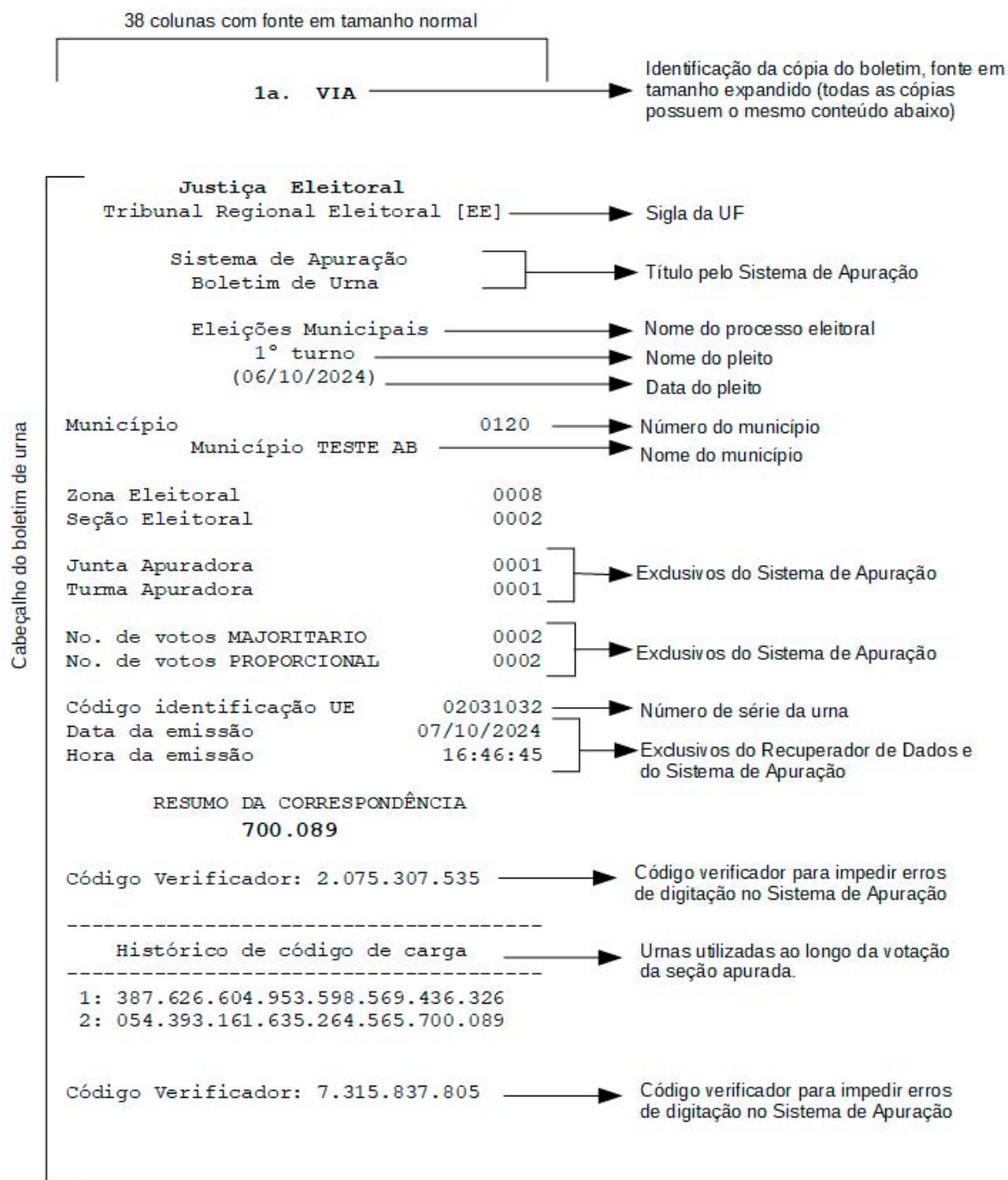
MINISTÉRIO PÚBLICO:

FISCAIS:



Assinaturas para o Recuperador de
Dados e para o Sistema de Apuração

Em seguida, a visão do cabeçalho do BU impresso pelo Sistema de Apuração, quando há a realização de duas eleições no mesmo pleito e seu respectivo QR Code. O corpo do boletim foi omitido devido a sua semelhança com o Boletim do Software de Votação.





QR Code impresso

ASSINATURA QR CODE:
A5BFB1A8A1ABFE2171DF515F9AE62D2ABC84B3
81A2455CEF23AB4978AF9D2FB9AC5C9B1285F1
C04A1235402170F72445A618BB7F9E1E97C64F
FB1AA96DB5190C

Assinatura do conteúdo do QR Code (igual
ao codificado dentro do QR Code)

=====SIMULADO=====

Código de identificação da carga
054.393.161.635.264.565.700.089

Número único que vincula a seção eleitoral
à urna eletrônica

Ver: 9.20.0.0

Versão do software da urna (número)

o conteúdo deste BU poderá ser
conferido no endereço
resultados.tse.jus.br

Local onde o boletim será disponibilizado
para conferência

ASSINATURAS:

Assinaturas de próprio punho das pessoas
listadas no momento de fechamento da urna

PRESIDENTE DA JUNTA:

COMPONENTES DA JUNTA:

MINISTÉRIO PÚBLICO:

FISCAIS:

Assinaturas para o Recuperador de
Dados e para o Sistema de Apuração



3. POR QUE QR CODE E COMO ELE FOI IMPLANTADO

Recentemente, a tecnologia QR Code tornou-se universal, pois está presente nas mais variadas mídias e é facilmente utilizada com o suporte dos mais variados dispositivos, sobretudo nos *smartphones*. A grande capacidade de representação de dados, aliada ao forte suporte nos dispositivos móveis, faz do QR Code uma escolha natural para a digitalização rápida do BU.

Devido às limitações da impressora da urna (impressora térmica capaz de imprimir imagens monocromáticas de baixa resolução), o QR Code impresso está limitado à representação de até 1.100 caracteres no modo de entrada alfanumérico². Dessa forma, é possível trabalhar com uma taxa de compressão adequada ao mesmo tempo em que é possível utilizar um formato de representação que seja legível por pessoas que usam aplicativos de leitura genéricos. Essa característica é importante para o fácil desenvolvimento de aplicativos específicos de leitura do BU por pessoas com pouco ou nenhum conhecimento do processo eleitoral brasileiro.

A utilização do modo de entrada alfanumérico restringe a utilização de nomes no conteúdo codificado no QR Code, uma vez que a língua portuguesa é rica em nomes com caracteres acentuados. O armazenamento de nomes no QR Code (nomes de candidatas, candidatos, cargos e eleições) também implicaria a utilização de mais imagens para representar todo o boletim, uma vez que demandaria o modo de entrada binário. Dessa forma, todos os nomes foram suprimidos. Ainda assim, os BUs podem ser muito extensos, chegando a apresentar até mesmo quatro QR Codes, devido ao grande número de candidaturas.

O VOTA utiliza a biblioteca libqrencode³ para a geração de QR Codes.

4. FORMATO DE REPRESENTAÇÃO DO BOLETIM DE URNA (BU)

O BU é codificado no QR Code, utilizando somente os caracteres previstos no modo de entrada alfanumérico (letras, números, alguns sinais de pontuação e espaço em branco). A partir daí, foi criada uma estrutura simples do tipo “chave e valor”. Todos os registros estão na mesma linha, com a chave separada do valor pelo caractere de dois-pontos, e os registros separados por espaço em branco. Todo QR Code possui três seções: cabeçalho, conteúdo do boletim e segurança.

Cada QR Code está limitado a 1.100 caracteres, incluindo todas as três seções. A seção de conteúdo pode ser dividida para que o limite máximo de cada QR Code não seja ultrapassado. Isso é feito no último espaço em branco antes da posição de quebra, de modo que um registro fique dividido entre dois QR Codes, retirando-se esse espaço em branco. Ao remontar integralmente a seção de conteúdo do boletim, é necessário adicionar novamente esse espaço em branco, para fins de cálculo de *hash* e assinatura digital.

² Disponível em: <https://en.wikipedia.org/wiki/QR_code#Storage>.

³ Disponível em: <<https://github.com/fukuchi/libqrencode>>.



4.1. Cabeçalho

Campo	Descrição
QRBU:n:x	Marca de início dos dados.n = índice do QR Code em uma sequência de QR Codes.x = quantidade total de QR Codes.
VRQR:n.y	Número da versão do formato da representação do boletim de urna.n = número de ciclos eleitorais desde sua implementação.y = número de revisões do formato dentro de um ciclo.
VRCH:nnnn...	Número da versão da chave utilizada para assinar o conteúdo do QR Code.

4.2. Conteúdo do boletim

- Cabeçalho do Boletim de Urna

Campo	Descrição
ORIG:xxxx	Origem do boletim de urna (VOTA, RED ou SA).
ORLC:xxx	Origem da configuração do processo eleitoral (LEG – eleição legal oficial; COM – eleição comunitária).
PROC:nnnnn	Número do processo eleitoral.
DTPL:aaaammdd	Data do pleito.
PLEI:nnnnn	Número do pleito.
TURN:n	Número do turno (1 – primeiro turno; 2 – segundo turno).
FASE:x	Fase dos dados (O – oficial; S – simulado; T – treinamento).
UNFE:xx	Sigla da UF. No caso de eleição no exterior, a sigla será ZZ.
MUNI:nnnnn	Número do município.
ZONA:nnnn	Número da zona eleitoral.
SECA:nnnn	Número da seção eleitoral.
AGRE:nnnn.nnnn...	Número das seções agregadas separadas por um ponto.
IDUE:nnnn...	Número de série da urna.
IDCA:nnnn...	Código de identificação da carga (24 dígitos).
HIQT:n	Quantidade de códigos de carga.
HICA:n:nnnn...	Histórico de códigos de carga (sequência de carga:código de identificação de carga).
VERS:xxxx...	Texto de tamanho variável com a versão do <i>software</i> da urna (somente números e pontos).



- Cabeçalho do Boletim de Urna – Campos exclusivos do Software de Votação (VOTA) e do Recuperador de Dados (RED)

Campo	Descrição
LOCA:nnnn	Número do local de votação.
APTO:nnnn	Total de eleitores aptos.
APTS:nnnn	Total de eleitores aptos originários da seção.
APTT:nnnn	Total de eleitores aptos transferidos temporariamente para a seção.
COMP:nnnn	Quantidade de eleitores que compareceram para votar.
FALT:nnnn	Quantidade de eleitores faltosos.
HBBM:nnnn	Total de eleitores habilitados biometricamente.
HBBG:nnnn	Total de eleitores com biometria não reconhecida e habilitados por ano de nascimento.
HBSB:nnnn	Total de eleitores sem biometria, habilitados por ano de nascimento.
DTAB:aaaammdd	Data da abertura da urna.
HRAB:hhmmss	Hora da abertura da urna.
DTFC:aaaammdd	Data do fechamento da urna.
HRFC:hhmmss	Hora do fechamento da urna.

- Cabeçalho do Boletim de Urna – Campos exclusivos do Sistema de Apuração (SA)

Campo	Descrição
JUNT:nnnn	Número da junta apuradora.
TURM:nnnn	Número da turma apuradora.

- Cabeçalho do Boletim de Urna – Campos exclusivos do Sistema de Apuração (SA) e do Recuperador de Dados (RED)

Campo	Descrição
DTEM:aaaammdd	Data de emissão do boletim de urna.
HREM:hhmmss	Hora de emissão do boletim de urna.

- Cabeçalho da eleição

É incluído para cada eleição.

Campo	Descrição
IDEL:nnnnn	Código da eleição.
MAJO:nnnn	Número de votos nos cargos majoritários – campo exclusivo do Sistema de Apuração (SA).
PROP:nnnn	Número de votos nos cargos proporcionais – campo exclusivo do Sistema de Apuração (SA).



- Cabeçalho do cargo

É incluído para cada cargo sendo apurado. A partir dele, é possível remontar o cargo e o tipo do cargo.

Campo	Descrição
CARG:nn	Código do cargo.
TIPO:n	Tipo: 0 – Majoritário; 1 – Proporcional; 2 – Consulta.
VERC:n	Versão do pacote de dados de candidatos/consulta.

- Cabeçalho do partido

É incluído para cada partido com votação para o cargo. A partir dele, é possível remontar a abertura e o fechamento dos votos para o partido. Opcional – Só incluído para cargos proporcionais.

Campo	Descrição
PART:nn	Número do partido.
LEGP:nnnn	Quantidade de votos de legenda para o partido.
TOTP:nnnn	Total de votos apurados para o partido.

- Votação da candidata, do candidato ou da resposta

É incluída para cada candidata, candidato ou resposta que recebeu votos. São agrupados pelo cargo (majoritário ou consulta) ou pelo partido (proporcional).

Campo	Descrição
cccc:nnnn	Número do candidato ou resposta, seguido da quantidade de votos que recebeu.

- Resumo do cargo

É incluído para cada cargo sendo apurado. A partir dele, é possível remontar a abertura e o fechamento dos votos para o cargo.

Campo	Descrição
APTA:nnnn	Total de eleitores aptos para votar no cargo.
APTS:nnnn	Total de eleitores aptos para votar no cargo originários da seção.
APTT:nnnn	Total de eleitores aptos para votar no cargo transferidos temporariamente para a seção.
CSEC:nnnn	Quantidade de comparecimento no cargo sem candidatos.
NOMI:nnnn	Quantidade de votos nominais para o cargo.
LEGC:nnnn	Quantidade de votos de legenda para o cargo. Opcional – só incluído para cargos proporcionais.
BRAN:nnnn	Quantidade de votos em branco para o cargo.
NULO:nnnn	Quantidade de votos nulos para o cargo.
TOTC:nnnn	Total de votos apurados para o cargo.



4.3. Segurança

Campo	Descrição
HASH:xxxxxx...	Hash da seção de conteúdo do boletim. Ao final de cada QR Code, virá um <i>hash</i> cumulativo aos dados de todos os anteriores, o que permite a verificação da leitura em sequência. O cálculo é feito com SHA-512, codificado em hexadecimal.
ASSI:xxxxxx...	Assinatura digital Ed25519 a partir do último <i>hash</i> (incluído somente no último QR Code). Codificado em hexadecimal e também impresso no boletim em papel.


5. CÓDIGO DOS CARGOS

Para fins de identificação dos cargos, a partir dos seus códigos encontrados no QR Code do BU, segue a lista de cargos e seus respectivos códigos.

Cargo	Descrição
Presidente	1
Governador	3
Senador	5
Deputado Federal	6
Deputado Estadual	7
Deputado Distrital	8
Conselheiro Distrital	9
Prefeito	11
Vereador	13


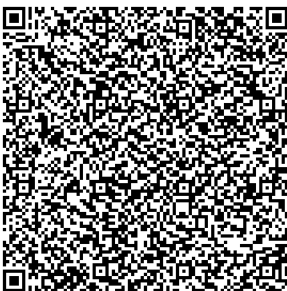

5.1. Exemplos

BU “pequeno”, os cargos para prefeito e vereador, todos os cargos com diversas candidatas e com diversos candidatos, com comparecimento de duas eleitoras ou de dois eleitores.

Imagem QrCode	Dados da imagem
 <p>ASSINATURA QR CODE: B2FA068D49111BA3A61DA0DC44334F8EC4159 8C73DE90B8E22AA64DAB8C10AA083FD0737B47 560B3C6C837D0F24044ABB18DD5A4D2BC66884 DB57BFCFA40F906</p>	<p>QRBU:1:1 VRQR:1.5 VRCH:20240507 ORIG:VOTA ORLC:LEG PROC:1000 DTPL:20241006 PLEI:1100 TURN:1 FASE:S UNFE:AC MUNI:1120 ZONA:8 SECA:2 AGRE:3.4 IDUE:2031032 IDCA:387626604953598569436326 HIQT:1 HICA:1:387626604953598569436326 VERS:9.20.0.0 LOCA:1 APT0:144 APTS:144 APTT:0 COMP:2 FALT:142 HBBM:0 HBBG:0 HBSB:2 DTAB:20241006 HRAB:172113 DTFC:20241006 HRFC:172300 IDEL:1101 CARG:13 TIPO:1 VERC:202405101700 PART:93 93001:1 LEGP:0 TOTP:1 APTA:144 APTS:144 APTT:0 NOMI:1 LEGC:0 BRAN:1 NULO:0 TOTC:2 CARG:11 TIPO:0 VERC:202405101700 92:1 APTA:144 APTS:144 APTT:0 NOMI:1 BRAN:0NULO:1 TOTC:2 HASH:57D17C50037 E7E4C624468438AE77BEA6562076A20CD454FE30EAD413F7D6174ADE59D0D970 13BD8F9F50316D766D3670B57FBB7D396C08DD4C4D9250E7B05FC ASSI:B2FA06 8D49111BA3A61DA0DC44334F8EC41598C73DE90B8E22AA64DAB8C 10AA083FD0737B47560B3C6C837D0F24044ABB18DD5A4D2BC66884DB5 7BFCFA40F906</p>



BU “grande”, com mais de uma imagem, os cargos para prefeito e vereador, todos os cargos com diversas candidatas ou com diversos candidatos, com comparecimento de 504 eleitoras, eleitores e votos em candidatas ou em candidatos diferentes para o cargo de vereador. Para representar as informações contidas na votação desse exemplo, foram necessárias quatro imagens de QR Codes.

Imagem QrCode	Dados de cada imagem
 <p>QrCode 1 de 4</p>	<p>QRBU:1:4 VRQR:1.5 VRCH:20240507 ORIG:VOTA ORLC:LEG PROC: 1000 DTPL:20241006 PLEI:1100 TURN:1 FASE:S UNFE:ACMUNI:1392 ZONA:9 SECA:22 IDUE:2033200 IDCA:216820571350570928893711 HIQT:1 HICA:1:216820571350570928893711 VERS:9.21.0.0 LOCA:4 APT0:559 APTS:559 APTT:0 COMP:504 FALT:55 DTAB:20241006 HRAB:091502 DTFC:20241006 HRFC:170042 IDEL:1101 CARG:13 TIPO:1 VERC:202 406131529 PART:91 91001:1 91002:1 91003:4 91004:1 91005:3 91006:3 91007:1 91009:1 91010:1 91011:1 91012:3 91013:1 91014:2 91015:2 91018:1 91020:3 91022:5 91024:2 91025:2 91026:3 91027:3 91028:2 91029:1 91030:2 91031:1 91032:1 91033:2 91034:1 91035:1 91036:1 91037:2 91038:2 91039:5 91040:3 91043:1 91044:4 91045:1 91046:3 91047:2 91048:1 91049:2 91050:1 91051:3 91052:2 91054:2 91055:2 91056:3 91057:1 91059:3 LEGP:0 TOTP:99 PART:92 92001:2 92002:3 92003:2 92004:3 92005:2 92006:2 92007:1 HASH:C84EAF7AEC9D9 5CD157B5F00206C708B0E6BB67226098903B0050F12D3BEFF 79B7EF6025FBA22 54E388E264511816BC270EB8701FC9455170F D905BFC6E19628</p>
 <p>QrCode 2 de 4</p>	<p>QRBU:2:4 VRQR:1.5 VRCH:20240507 92008:6 92009:2 92010:1 92011:2 92013:1 92014:1 92015:5 92017:3 92018:1 92019:4 92020:3 92021:1 92022:1 92023:1 92024:3 92025:1 92026:2 92027:3 92030:4 92032:2 92033:2 92034:2 92035:1 92036:3 92037:2 92038:1 92039:6 92040:1 92041:1 92042:2 92043:4 92044:2 92047:3 92048:4 92049:1 92050:1 92051:1 92053:2 92054:1 92055:3 92056:1 92057:2 92058:2 92059:2 LEGP:0 TOTP:112 PART:93 93001:2 93002:2 93003:2 93005:2 93006:3 93007:2 93008:5 93009:1 93010:1 93011:2 93012:2 93013:3 93014:1 93015:2 93017:3 93018:1 93019:2 93020:3 93022:1 93023:1 93024:1 93025:5 93026:3 93027:2 93028:1 93029:2 93030:2 93031:1 93032:1 93033:4 93034:2 93035:2 93036:1 93037:1 93039:1 93040:2 93041:1 93042:2 93043:1 93044:1 93045:1 93046:2 93047:1 93048:5 93049:2 93050:1 93052:3 93053:4 93054:2 93055:1 93056:2 93057:2 93058:2 93059:1 LEGP:1 HASH:643D452C83DBADB591895D9D2ACEF3F6E70 6E3A2E67D53671812BADEF002CC0AE9D16C0DC7BD5F2BF9FDA5F6E6 16B04974276843375B46D15CF88300FEC7D96</p>
 <p>QrCode 3 de 4</p>	<p>QRBU:3:4 VRQR:1.5 VRCH:20240507 TOTP:107 PART:94 94001:2 94003:1 94004:3 94005:3 94007:3 94008:1 94010:1 94011:2 94012:2 94013:5 94014:2 94015:2 94017:1 94018:3 94019:1 94020:1 94021:1 94022:1 94023:2 94024:1 94025:2 94026:2 94027:2 94028:2 94029:1 94030:3 94031:2 94032:1 94033:1 94034:3 94035:1 94037:1 94038:3 94039:2 94040:3 94041:1 94042:1 94044:1 94045:1 94046:1 94047:2 94048:1 94050:3 94052:1 94053:1 94054:1 94056:2 94057:2 94058:1 LEGP:1 TOTP:87 PART:95 95001:3 95002:3 95016:1 95017:2 95018:1 95022:1 95023:2 95024:2 95025:1 95026:1 95027:1 95028:2 95029:3 95030:3 95031:3 95032:2 95033:2 95035:1 95036:1 95037:1 95038:2 95040:4 95041:2 95043:2 95044:1 95045:3 95046:3 95047:1 95048:2 95049:3 95050:1 95051:2 95052:1 95053:1 95054:2 95056:1 HASH:FA3D6F3A7 62B4F03F0813C7AC06E6230017FAB80AE7333098E5255F5879A3F 1EEDB126D1AAA5F 0188131261961F4F041F4BE06F296143358 9EB9AA51FBF8C484</p>



QrCode 4 de 4 **ASSINATURA:**
 154D5E3ABD3567C3
 53D144A324BE4D2EFBDB71
 6685F3155AB07C2105B3774FCE3
 262FDCE50CE5FBE95828EC19
 141991C04FAA0A91A2C54
 CDC33E6D0716F1190E

QRBU:4:4 VRQR:1.5 VRCH:20240507 95058:1 95059:2 LEGP:3
 TOTP:99 APTA:559 APTS:559 APTT:0 NOMI:499 LEGC:5
 BRAN:0 NULO:0 TOTC:504 CARG:11 TIPO:0 VERC:202406
 131529 91:102 92:105 93:111 94:95 95:91 APTA:559 APTS:
 559 APTT:0 NOMI:504 BRAN:0 NULO:0 TOTC:504HASH:27
 FF0E01FB973621CAD76FF624B71A396AA858E57
 24179A0DA3CC160811F5BF550D85024C75CA54686
 901FBC12695D21C2EBDA46EA7D1B2593B4459EAF0BDEF6
ASSI:154D5E3ABD3567C353D144A324BE4D2EFBDB7166
 85F3155AB07C2105B3774FCE3262FDCE5 0CE5FBE9582
 8EC19141991C04FAA0A91A2C54CDC33E6D0716F1190E

6. ASSINATURA DIGITAL

Para a assinatura do conteúdo do BU codificado no QR Code foi escolhido o algoritmo de chave pública Ed25519⁴ e sua configuração para assinatura digital EdDSA. Ed25519 é um algoritmo de curvas elípticas, moderno, de alto desempenho, elevado nível de segurança e que possui implementações resistentes a ataques do tipo *side-channel*. Embora ainda esteja em processo de padronização⁵, o Ed25519 conta com uma adoção cada vez maior pela comunidade⁶, já presente em diversas ferramentas de segurança e com implementações de código aberto para as mais variadas linguagens de programação e plataformas.

O *software* da urna utiliza a biblioteca OpenSSL⁷ para a geração de assinaturas e pares-chaves. Devido às limitações de espaço do QR Code e a sua aplicação em dispositivos móveis, um benefício importante do Ed25519 é o tamanho de chave (256 *bits*) e de assinatura reduzidos (512 *bits*).

Após a Cerimônia de Lacração e Assinatura Digital dos Sistemas Eleitorais, as chaves públicas Ed25519, utilizadas pelo *software* da urna, serão publicadas na internet. É gerado um par de chaves por Unidade da Federação (UF). Os aplicativos móveis precisarão dessas chaves para a validação da assinatura do conteúdo do boletim nos QR Codes.

É importante destacar que o algoritmo de assinatura digital utilizado para os QR Codes é de domínio público e por isso foi escolhido para essa aplicação. A assinatura digital empregada na validação dos arquivos de resultado da urna eletrônica pelo sistema de totalização da Justiça Eleitoral utiliza um algoritmo Estado, conforme estabelecido em norma específica⁸.

4 Disponível em: <<http://ed25519.cr.yp.to/>>.

5 Disponível em: <<https://tools.ietf.org/html/draft-josefsson-eddsa-ed25519-02>>.

6 Disponível em: <<http://ianix.com/pub/ed25519-deployment.html>>.

7 Disponível em: <<https://www.openssl.org/>>.

8 Disponível em: <http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf>.



6.1. Formação da assinatura

A assinatura é realizada a partir do *hash* do último QR Code impresso, porém esse último *hash* é calculado a partir dos *hashes* dos demais QR Codes cumulativamente. Por exemplo:

```
QRBU:1:N VRQR:1.5 VRCH:nnnnnnnn [dados1] HASH:hash([dados1]),

QRBU:2:N VRQR:1.5 VRCH: nnnnnnnnn [dados2] HASH:hash([conteúdo1] +
[dados2]),
sendo conteúdo1 = [dados1] HASH:hash1

QRBU:3:N VRQR:1.5 VRCH: nnnnnnnnn [dados3] HASH:hash([conteúdo2] +
[dados3]),
sendo conteúdo2 = [dados1] HASH:hash1 [dados2] HASH:hash2
...

QRBU:N:N VRQR:1.5 VRCH: nnnnnnnnn [dadosN] HASH:hash([conteúdo(N-1)] +
[dadosN]),
sendo conteúdo(N-1) = [dados1] HASH:hash1 [dados2] HASH:hash2 ...
[dados(N-1)] HASH:hash(N-1)

ASSI:assinatura(hashN),
sendo hashN = hash([conteúdo(N-1)] + [dadosN])
```

Os exemplos apresentados neste manual, que possuem assinatura válida, podem ser verificados com a chave pública específica, do tipo Ed25519 (algoritmo EdDSA), de 256 *bits* e em hexadecimal:

```
3c8dd2914fc8b20bd80b09744867684c051145e3f8b887d28af3d23a17a843dd
```

6.2. Instruções para a verificação de assinatura digital e exemplos de código

- Verificação de assinatura do QR Code

No Manual para a Construção de Aplicativos de Leitura, já foi feita uma breve explicação sobre o método de assinatura digital EdDSA empregado no QR Code. Naquela documentação, também há a descrição do algoritmo de composição da mensagem assinada e exemplos válidos para verificação. Agora são dados mais detalhes sobre o acesso às chaves públicas e um exemplo de código-fonte C++ para a verificação de assinatura.

As chaves públicas estarão disponíveis no endereço:

```
<URL_BASE/[VERSAO_CHAVE]/[LEGAL|COMUNITARIA]/[O|S][SIGLA_UF]qrcode.pub>
```

Em que:

URL_BASE - <http://qrnodenobu.tse.jus.br/tse.qrcodibu>

VERSAO_CHAVE – Versão das chaves, encontrada no QR Code

[] – Indica um conjunto fixo de valores

| – Indica uma opção dentro de um conjunto de possibilidades



SIGLA_UF – Sigla da UF, minúsculo. No caso das eleições realizadas no exterior, a sigla da UF será zz.

A informação LEGAL ou COMUNITARIA corresponde ao tipo da eleição.

Haverá uma nova versão das chaves para as eleições de 2024. Para os BUs utilizados como exemplo neste documento, a versão das chaves utilizadas foi 20240507.

Exemplo: para validação das assinaturas dos BUs utilizados como exemplo neste documento foi utilizada a chave seguinte:

<<http://qrcomobu.tse.jus.br/tse.qrcodebu/20240507/LEGAL/sacqrcode.pub>>

Dessa forma, com as informações encontradas no QR Code no BU, é possível carregar a chave pública correta. Os arquivos são binários e contêm unicamente os *bytes* da chave pública.

A seguir, um exemplo de código C++ que utiliza a libsodium⁹ para a validação da assinatura digital de um QR Code. A função `TesteValidaAssinatura()` faz a validação da assinatura digital.

```
#include <fstream>
#include <cctype>
#include <algorithm>
#include <sodium.h>

int hexValue(int c) {
    if (c >= '0' && c <= '9') return c - '0';
    if (c >= 'A' && c <= 'F') return c - 'A' + 10;
    if (c >= 'a' && c <= 'f') return c - 'a' + 10;
    return -1;
}

std::vector<unsigned char> HexToBytes(const std::string & value) {
    if (value.empty() || not std::all_of(value.begin(), value.end(),
::isxdigit)) {
        throw std::logic_error("Erro");
    }

    std::vector<unsigned char> bytes;
    for (int i=0, n = value.size(); i< n-1; i+=2) {
        int x1 = hexValue(value[i]);
        int x2 = hexValue(value[i+1]);
        if (x1 >= 0 && x2 >= 0) {
            bytes.push_back(x1*16 + x2);
        }
    }
    return bytes;
}
```

9 Disponível em: <https://github.com/jedisct1/libsodium> <https://github.com/jedisct1/libsodium>.



```

std::vector<unsigned char> RecuperaConteudoDaChave(const std::string &
chavePublica) {
    std::ifstream ifs(chavePublica.c_str(), std::ios::binary|
std::ios::ate);
    std::ifstream::pos_type pos = ifs.tellg();

    std::vector<char> resultado(pos);

    ifs.seekg(0, std::ios::beg);
    ifs.read(&resultado[0], pos);

    return std::vector<unsigned char>(resultado.begin(), resultado.end());
}

const std::vector<unsigned char> ConverteStringHexadecimalEmBytes(const
std::string & hexString) {
    return HexToBytes(hexString);
}

const std::vector<unsigned char> RecuperaConteudoDaChavePublica() {
    const std::string chavePublica = "sacqrcode.pub";
    return RecuperaConteudoDaChave(chavePublica);
}

int VerificaAssinatura(std::vector<unsigned char> & assinatura,
std::vector<unsigned char> & dadoASerValidado, std::vector<unsigned char>
& conteudoDaChavePublica) {
    std::vector<unsigned char> assinaturaComDadoAssinado(assinatura.
begin(), assinatura.end());
    assinaturaComDadoAssinado.insert(assinaturaComDadoAssinado.end(),
dadoASerValidado.begin(), dadoASerValidado.end());

    unsigned long long tamanhoDaMensagem = dadoASerValidado.size();
    return crypto_sign_open(dadoASerValidado.data(), &tamanhoDaMensagem,
assinaturaComDadoAssinado.data(), assinaturaComDadoAssinado.size(),
conteudoDaChavePublica.data());
}

void TesteValidaAssinatura() {
    const std::string conteudoASerValidado = "QRBU:1:1 VRQR:1.5
VRCH:20240507
ORIG:VOTA ORLC:LEG PROC:1000 DTPL:20241006 PLEI:1100 TURN:1 FASE:S
UNFE:AC MUNI:1120
ZONA:8 SECA:2 AGRE:3.4 IDUE:2031032 IDCA:387626604953598569436326

```




```

HIQT:1
HICA:1:387626604953598569436326 VERS:9.20.0.0 LOCA:1 APTO:144 APTS:144
APTT:0 COMP:2
FALT:142 HBBM:0 HBBG:0 HBSB:2 DTAB:20241006 HRAB:172113 DTFC:20241006
HRFC:172300
IDEL:1101 CARG:13 TIPO:1 VERC:202405101700 PART:93 93001:1 LEGP:0
TOTP:1 APTA:144
APTS:144 APTT:0 NOMI:1 LEGC:0 BRAN:1 NULO:0 TOTC:2 CARG:11 TIPO:0
VERC:202405101700
92:1 APTA:144 APTS:144 APTT:0 NOMI:1 BRAN:0 NULO:1 TOTC:2";
const std::string hashConteudoASerValidado =
"57D17C50037E7E4C624468438AE77BEA6562076A20CD454FE30EAD413
F7D6174ADE59D0D97013BD8F9F50316D766D3670B57FBB7D396C08DD4C4D9250E7B05FC";

std::vector<unsigned char> conteudoDaChavePublica =
RecuperaConteudoDaChavePublica();
std::vector<unsigned char> assinatura =
ConverteStringHexadecimalEmBytes("B2FA068D49111BA3A61DA0DC44334F8EC41598C73
DE90B8E22AA64DAB8C10AA083FD0737B47560B3C6C837D0F24044ABB18DD5A4D2BC66884DB5
7BFCFA40F906");
std::vector<unsigned char> dadoASerValidado =
ConverteStringHexadecimalEmBytes(hashConteudoASerValidado);
int resultadoDaVerificacao = VerificaAssinatura(assinatura,
dadoASerValidado, conteudoDaChavePublica);

if (resultadoDaVerificacao == 0) {
    printf("Assinatura OK.\n");
} else {
    printf("Erro na assinatura.\n");
}
}

```



7. COMPLEMENTO DOS DADOS – NOMES DAS CANDIDATAS, DOS CANDIDATOS, DOS CARGOS E DAS ELEIÇÕES

Conforme pode ser visto na descrição do BU impresso, o relatório conta com uma série de nomes: processo eleitoral, pleito, eleições, municípios, cargos, partidos, candidatas e candidatos. A inclusão desses nomes no QR Code tornaria necessária a utilização de um número muito maior de códigos de barras. Dessa forma, os nomes foram omitidos no QR Code e, em seu lugar, foram usados códigos para referência.

Após a conclusão da preparação das urnas, às vésperas da realização do pleito, a Justiça Eleitoral publicará na internet um conjunto de arquivos com os nomes do processo eleitoral, pleito, eleições, municípios, cargos, partidos, candidatas e candidatos. A partir dos códigos presentes no QR Code, será possível obter os respectivos nomes.

Esse arquivo de complemento dos dados tem o formato JSON. Um exemplo desse arquivo é apresentado a seguir. Ele inclui a assinatura digital, que também utiliza EdDSA (o mesmo algoritmo utilizado no QR Code, mas com chaves diferentes).

Os arquivos serão disponibilizados na internet e poderão ser baixados a partir do seguinte endereço:

http://qrcodenobu.tse.jus.br/json-bu/**fase**/**idProcesso**/**FpppppUFMMMMM**-qbu.js

fase – Fase dos dados por extenso, minúsculo (oficial; simulado; treinamento)

idProcesso – Número do processo eleitoral

F – Fase dos dados (o – oficial; s – simulado; t – treinamento)

ppppp – Número do pleito, com zeros à esquerda

UF – Sigla da UF, minúsculo

MMMMM – Número do município, com zeros à esquerda

7.1. Schema JSON

```
/**
 * Contrato para os dados de complemento do QR Code do boletim de urna.
 */
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "QRCode-BU",
  "description": "Contrato para os dados de complemento do QRCode do boletim de urna.",
  "type": "object",
  "properties": {
    "processoEleitoral": {
      "$ref": "#/definitions/processoEleitoral"
    },
    "assinatura": {
      "description": "A assinatura do arquivo.",
      "type": "string"
    }
  }
}
```



```

},
"required": ["processoEleitoral", "assinatura"],
"definitions": {
  /**
   * Objeto com os dados do processo.
   */
  "processoEleitoral": {
    "description": "Objeto com os dados do processo.",
    "type": "object",
    "properties": {
      "codigo": {
        "description": "O código do processo.",
        "type": "integer",
        "minimum": 0,
        "maximum": 99999
      },
      "nome": {
        "description": "O nome do processo.",
        "type": "string"
      },
      "pleito": {
        "$ref": "#/definitions/pleito"
      },
      "municipio": {
        "$ref": "#/definitions/municipio"
      },
      "eleicoes": {
        "description": "Lista de eleições do boletim de urna.",
        "type": "array",
        "items": {
          "$ref": "#/definitions/eleicao"
        }
      },
      "consultasPopulares": {
        "description": "Lista de consultas populares do boletim
de urna.",
        "type": "array",
        "items": {
          "$ref": "#/definitions/consultaPopular"
        }
      }
    },
    "required": ["codigo", "nome", "pleito", "municipio"]
  },
  /**
   * O pleito das eleições.
   */
  "pleito": {
    "description": "O pleito das eleições.",
    "type": "object",

```



```

    "properties": {
      "codigo": {
        "description": "O código do pleito.",
        "type": "integer",
        "minimum": 0,
        "maximum": 99999
      },
      "nome": {
        "description": "O nome do pleito.",
        "type": "string"
      },
      "data": {
        "description": "A data do pleito.",
        "type": "string"
      }
    },
    "required": ["codigo", "nome", "data"]
  },
  /**
   * Os dados do município do boletim de urna.
   */
  "municipio": {
    "description": "Os dados do município do boletim de urna.",
    "type": "object",
    "properties": {
      "numero": {
        "description": "O número do município.",
        "type": "integer",
        "minimum": 0,
        "maximum": 99999
      },
      "nome": {
        "description": "O nome do município.",
        "type": "string"
      }
    },
    "required": ["numero", "nome"]
  },
  /**
   * Objeto com os dados de um partido.
   */
  "partido": {
    "description": "Objeto com os dados de um partido.",
    "type": "object",
    "properties": {
      "numero": {
        "description": "O número do partido.",
        "type": "integer",
        "minimum": 0,
        "maximum": 99
      }
    }
  }
}

```



```

    },
    "sigla": {
        "description": "A sigla do partido.",
        "type": "string"
    },
    "nome": {
        "description": "O nome do partido.",
        "type": "string"
    }
},
"required": ["numero", "sigla", "nome"]
},
/**
 * Objeto com os dados do cargo.
 */
"cargo": {
    "description": "Objeto com os dados do cargo.",
    "type": "object",
    "properties": {
        "codigo": {
            "description": "O código do cargo.",
            "type": "integer",
            "minimum": 0,
            "maximum": 99
        },
        "versao": {
            "description": "A versão do arquivo do 'Candidaturas'
utilizado na geração.",
            "type": "string"
        },
        "nomeNeutro": {
            "description": "O nome neutro do cargo.",
            "type": "string"
        },
        "nomeMasculino": {
            "description": "O nome masculino do cargo.",
            "type": "string"
        },
        "nomeFeminino": {
            "description": "O nome feminino do cargo.",
            "type": "string"
        },
        "nomeAbreviado": {
            "description": "O nome abreviado do cargo.",
            "type": "string"
        }
    },
    "required": ["codigo", "versao", "nomeNeutro", "nomeMasculino",
"nomeFeminino", "nomeAbreviado"];
},

```



```

/**
 * Objeto com os dados do candidato.
 */
"candidato": {
  "description": "Objeto com os dados do candidato.",
  "type": "object",
  "properties": {
    "codigo": {
      "description": "O código do candidato.",
      "type": "integer"
    },
    "nome": {
      "description": "O nome do candidato.",
      "type": "string"
    }
  },
  "required": ["codigo", "nome"]
},
/**
 * Objeto com os dados da candidatura.
 */
"candidatura": {
  "description": "Objeto com os dados da candidatura.",
  "type": "object",
  "properties": {
    "numero": {
      "description": "O número da candidatura.",
      "type": "integer",
      "minimum": 0,
      "maximum": 99999
    },
    "titular": {
      "$ref": "#/definitions/candidato"
    },
    "suplentes": {
      "description": "Lista de vices e suplentes.",
      "type": "array",
      "items": {
        "$ref": "#/definitions/candidato"
      }
    }
  },
  "required": ["numero", "titular"]
},
/**
 * Lista de candidaturas de um partido.
 */
"candidaturasPorPartido": {
  "description": "Lista de candidaturas de um partido.",
  "type": "object",

```



```

    "properties": {
      "partido": {
        "$ref": "#/definitions/partido"
      },
      "candidaturas": {
        "description": "Lista de candidaturas do partido.",
        "type": "array",
        "items": {
          "$ref": "#/definitions/candidatura"
        }
      }
    },
    "required": ["partido", "candidaturas"]
  },
  /**
   * Lista de partidos de um cargo.
   */
  "partidosPorCargo": {
    "description": "Lista de partidos de um cargo.",
    "type": "object",
    "properties": {
      "cargo": {
        "$ref": "#/definitions/cargo"
      },
      "candidaturasPorPartidos": {
        "description": "Lista de candidaturas e partidos.",
        "type": "array",
        "items": {
          "$ref": "#/definitions/candidaturasPorPartido"
        }
      }
    },
    "required": ["cargo", "candidaturasPorPartidos"]
  },
  /**
   * Objeto com os dados de uma eleição.
   */
  "eleicao": {
    "description": "Objeto com os dados de uma eleição.",
    "type": "object",
    "properties": {
      "codigo": {
        "description": "O código da eleição.",
        "type": "integer",
        "minimum": 0,
        "maximum": 99999
      },
      "nome": {
        "description": "O nome da eleição.",
        "type": "string"
      }
    }
  }
}

```



```

    },
    "partidosPorCargos": {
        "description": "A data do pleito.",
        "type": "array",
        "items": {
            "$ref": "#/definitions/partidosPorCargo"
        }
    }
},
"required": ["codigo", "nome", "partidosPorCargos"]
},
/**
 * Objeto com os dados de uma resposta.
 */
"resposta": {
    "description": "Objeto com os dados de uma resposta.",
    "type": "object",
    "properties": {
        "numero": {
            "description": "O número da resposta.",
            "type": "integer",
            "minimum": 0,
            "maximum": 99
        },
        "descricao": {
            "description": "A descrição da resposta.",
            "type": "string"
        }
    },
    "required": ["numero", "descricao"]
},
/**
 * Objeto com os dados de uma pergunta.
 */
"pergunta": {
    "description": "Objeto com os dados de uma pergunta.",
    "type": "object",
    "properties": {
        "codigo": {
            "description": "O código da pergunta.",
            "type": "integer",
            "minimum": 0,
            "maximum": 99
        },
        "descricao": {
            "description": "A descrição da pergunta.",
            "type": "string"
        },
        "versao": {
            "description": "A versão do arquivo do Configurador de

```



```

Eleições utilizado.",
    "type": "string"
  },
  "respostas": {
    "description": "Lista de respostas da pergunta.",
    "type": "array",
    "items": {
      "$ref": "#/definitions/resposta"
    }
  }
},
"required": ["codigo", "descricao", "versao", "respostas"]
},
/**
 * Objeto com as perguntas de uma consulta popular.
 */
"consultaPopular": {
  "description": "Objeto com as perguntas de uma consulta
popular.",
  "type": "object",
  "properties": {
    "codigo": {
      "description": "O código da consulta popular.",
      "type": "integer",
      "minimum": 0,
      "maximum": 99999
    },
    "nome": {
      "description": "O nome da consulta popular.",
      "type": "string"
    },
    "perguntas": {
      "description": "Lista de perguntas da consulta.",
      "type": "array",
      "items": {
        "$ref": "#/definitions/pergunta"
      }
    }
  }
},
"required": ["codigo", "nome", "perguntas"]
}
}
}
}

```

Exemplo



```
{
  "assinatura": "7fa018741fc5838c0b74235a02fc639a5994e79272d99775e7681c6999
2c8898e3516ce1991f30d8260cf789763076cdb18d3575ea7ab39eeb8002e921366505",
  "processoEleitoral": {
    "codigo": 15000,
    "eleicoes": [
      {
        "codigo": 15103,
        "partidosPorCargos": [
          {
            "candidaturasPorPartidos": [
              {
                "partido": {
                  "sigla": "PEsp",
                  "numero": 91,
                  "nome": "Partido dos Esportes"
                },
                "candidaturas": [{
                  "numero": 91,
                  "suplentes": [{
                    "codigo": "47",
                    "nome": "Tênis"
                  }]
                },
                "titular": {
                  "codigo": "46",
                  "nome": "Volei"
                }
              }
            ]
          },
          {
            "partido": {
              "sigla": "PPartido Ritmos Musicais",
              "numero": 92,
              "nome": "Partido dos Ritmos Musicais"
            },
            "candidaturas": [{
              "numero": 92,
              "suplentes": [{
                "codigo": "49",
                "nome": "Pagode"
              }]
            },
            "titular": {
              "codigo": "48",
              "nome": "Forró"
            }
          }
        ]
      },
      {
        "partido": {
          "sigla": "PProf",
```



```
        "numero": 93,
        "nome": "Partido das Profissoes"
    },
    "candidaturas": [{
        "numero": 93,
        "suplentes": [{
            "codigo": "51",
            "nome": "Bibliotecária"
        }],
        "titular": {
            "codigo": "50",
            "nome": "Médica"
        }
    }],
},
{
    "partido": {
        "sigla": "PFest",
        "numero": 94,
        "nome": "Partido das Festas Populares"
    },
    "candidaturas": [{
        "numero": 94,
        "suplentes": [{
            "codigo": "53",
            "nome": "Natal"
        }],
        "titular": {
            "codigo": "52",
            "nome": "Dia da Independência do Brasil"
        }
    }],
},
{
    "partido": {
        "sigla": "PFolc",
        "numero": 95,
        "nome": "Partido do Folclore"
    },
    "candidaturas": [{
        "numero": 95,
        "suplentes": [{
            "codigo": "55",
            "nome": "Boitatá"
        }],
        "titular": {
            "codigo": "54",
            "nome": "Boto Cor-de-Rosa"
        }
    }],
}
```



```
    }
  ],
  "cargo": {
    "codigo": 11,
    "nomeMasculino": "Prefeito",
    "nomeFeminino": "Prefeita",
    "nomeNeutro": "Prefeito",
    "nomeAbreviado": "Pref.",
    "versao": "202405101700"
  }
},
{
  "candidaturasPorPartidos": [
    {
      "partido": {
        "sigla": "PEsp",
        "numero": 91,
        "nome": "Partido dos Esportes"
      },
      "candidaturas": [
        {
          "numero": 910001,
          "suplentes": [],
          "titular": {
            "codigo": "96",
            "nome": "Basquete"
          }
        },
        {
          "numero": 910002,
          "suplentes": [],
          "titular": {
            "codigo": "95",
            "nome": "Hipismo"
          }
        },
        {
          "numero": 910003,
          "suplentes": [],
          "titular": {
            "codigo": "98",
            "nome": "Patinação"
          }
        }
      ]
    },
    {
      "partido": {
        "sigla": "PPartido Ritmos Musicais",
        "numero": 92,
```



```
        "nome": "Partido dos Ritmos Musicais"
    },
    "candidaturas": [
        {
            "numero": 920001,
            "suplentes": [],
            "titular": {
                "codigo": "101",
                "nome": "Frevo"
            }
        },
        {
            "numero": 920002,
            "suplentes": [],
            "titular": {
                "codigo": "102",
                "nome": "Jazz"
            }
        },
        {
            "numero": 920003,
            "suplentes": [],
            "titular": {
                "codigo": "103",
                "nome": "Música Eletrônica"
            }
        }
    ],
    {
        "partido": {
            "sigla": "PProf",
            "numero": 93,
            "nome": "Partido das Profissoes"
        },
        "candidaturas": [
            {
                "numero": 930001,
                "suplentes": [],
                "titular": {
                    "codigo": "106",
                    "nome": "Garçom"
                }
            },
            {
                "numero": 930002,
                "suplentes": [],
                "titular": {
                    "codigo": "107",
                    "nome": "Motorista"
                }
            }
        ]
    }
```



```
    }
  },
  {
    "numero": 930003,
    "suplentes": [],
    "titular": {
      "codigo": "108",
      "nome": "Bombeira"
    }
  }
]
},
{
  "partido": {
    "sigla": "PFest",
    "numero": 94,
    "nome": "Partido das Festas Populares"
  },
  "candidaturas": [
    {
      "numero": 940001,
      "suplentes": [],
      "titular": {
        "codigo": "111",
        "nome": "Páscoa"
      }
    },
    {
      "numero": 940002,
      "suplentes": [],
      "titular": {
        "codigo": "112",
        "nome": "Réveillon"
      }
    },
    {
      "numero": 940003,
      "suplentes": [],
      "titular": {
        "codigo": "113",
        "nome": "Festa da Uva"
      }
    }
  ]
},
{
  "partido": {
    "sigla": "PFolc",
    "numero": 95,
    "nome": "Partido do Folclore"
```



```

        },
        "candidaturas": []
    }
],
"cargo": {
    "codigo": 13,
    "nomeMasculino": "Vereador",
    "nomeFeminino": "Vereadora",
    "nomeNeutro": "Vereador",
    "nomeAbreviado": "Ver.",
    "versao": "202405101700"
}
},
],
"nome": "Ele 2024-1º T Prefeitos e vereadores"
},
],
"consultasPopulares": [],
"municipio": {
    "numero": 1392,
    "nome": "RIO BRANCO"
},
"nome": "Cenário 15000 - Eleições Municipais 2024",
"pleito": {
    "codigo": 15100,
    "data": "06/10/2024",
    "nome": "1º Turno"
}
}
}
}

```

7.2. Verificação de assinatura do arquivo de complemento dos dados

O arquivo JSON – com os nomes do processo eleitoral, pleito, eleições, municípios, cargos, partidos, candidatas e candidatos – também possui uma assinatura digital EdDSA. A seguir, são dados mais detalhes sobre o acesso às chaves públicas e um exemplo de código-fonte Java para a verificação de assinatura.

A chave pública está disponível no endereço:

<<http://qrcodenobu.tse.jus.br/json-bu/s999999br-av.js>> para processos eleitorais em qualquer fase

O arquivo da chave está no formato JSON, com um único campo com a chave pública em hexadecimal.

A seguir, um exemplo de código Java utilizando a `ed25519-java`¹⁰ para a validação da assinatura digital de um arquivo de complemento. Para manipulação do arquivo de complemento e do arquivo de chave foi utilizada a biblioteca `JSON-java`¹¹.

Expandir código Java

¹⁰ Disponível em: <<https://github.com/str4d/ed25519-java>>.

¹¹ Disponível em: <<https://github.com/stleary/JSON-java>>.



```
import java.io.UnsupportedEncodingException;
import java.security.InvalidKeyException;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.security.SignatureException;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.X509EncodedKeySpec;
import net.i2p.crypto.eddsa.EdDSAEngine;
import net.i2p.crypto.eddsa.EdDSAPublicKey;
import net.i2p.crypto.eddsa.Utils;
import org.json.JSONObject;

public class ExemploAutenticacaoJson {

    public boolean autenticar(JSONObject complementoJson, String
chavePublica) throws SignatureException, InvalidKeyException,
NoSuchAlgorithmException, InvalidKeySpecException,
UnsupportedEncodingException {

        // Obtem a assinatura e a remove do objeto.
        String assinatura = complementoJson.getString("assinatura");
        complementoJson.remove("assinatura");

        // Carrega a chave publica e prepara o algoritmo.
        EdDSAEngine engine = new EdDSAEngine(MessageDigest.
getInstance("SHA-512"));
        X509EncodedKeySpec keySpec = new X509EncodedKeySpec(Utils.
hexToBytes(chavePublica));
        EdDSAPublicKey publicKey = new EdDSAPublicKey(keySpec);
        engine.initVerify(publicKey);

        // Converte o objeto em string e obtem os bytes.
        byte[] bytesJson = complementoJson.toString(2).getBytes("UTF-8");

        // Verifica a assinatura.
        return engine.verifyOneShot(bytesJson, Utils.
hexToBytes(assinatura));
    }
}
```



8. GLOSSÁRIO

1. **Abertura da urna:** momento em que a urna passa a aceitar a coleta de votos.
2. **Apuração:** contabilização do resultado de uma seção eleitoral.
3. **Boletim de Urna:** relatório impresso pela urna com o resultado apurado da seção eleitoral, apresentando os totais de votos nominais (somente para as candidatas e para os candidatos votados(as), total de votos por partido (no caso de cargos proporcionais) e votos brancos e nulos para cada cargo. Comumente chamado de BU.
4. **Cargo:** ocupação política que está em votação para o preenchimento de uma ou mais vagas ou um questionamento que está sendo submetido a consulta popular. São exemplos de cargos: presidente, governador, prefeito, vereador, senador, deputado federal, deputado estadual, deputado distrital; plebiscito para criação de um novo município ou estado, referendo para aprovação de uma lei.
5. **Cargo de consulta:** cargo correspondente a um plebiscito ou a um referendo, no qual o resultado corresponde à resposta mais votada.
6. **Cargo majoritário:** cargo para o qual o resultado é atribuído às candidatas e aos candidatos que receberam o maior número de votos. Presidente, governador, prefeito e senador são cargos majoritários.
7. **Cargo proporcional:** cargo para o qual o resultado é atribuído de acordo com uma fórmula que equaciona o total de vagas em disputa e o total de votos que as candidatas e os candidatos do partido ou da coligação receberam. Deputado federal, deputado estadual, deputado distrital e vereador são cargos proporcionais. A urna somente contabiliza os votos para cada candidata, candidato e partido nesse caso, pois a fórmula só pode ser aplicada na totalização.
8. **Cargo sem candidatas/candidatos:** cargo para o qual nenhuma candidata ou nenhum candidato se registrou, ou todas as candidatas e todos os candidatos tiveram o seu registro indeferido até o início da preparação das urnas, tornando-se inaptos(as) para a disputa.
9. **Cerimônia de Lacração e Assinatura Digital:** cerimônia pública, com a presença dos partidos políticos, da Ordem dos Advogados do Brasil (OAB) e do Ministério Público (MP), na qual são apresentados os códigos-fonte dos sistemas eleitorais, e estes são compilados. São gerados os *hashes* de cada arquivo produzido, os quais são publicados na internet para posterior verificação. Os sistemas também são assinados digitalmente para posterior validação. Somente os sistemas produzidos durante a cerimônia podem ser utilizados nas eleições.
10. **Código de identificação da carga:** número único que identifica uma urna preparada para a votação. O código de identificação da carga associado à identificação da urna (município, zona, seção e número de série do *hardware*) é chamado de *correspondência*.
11. **Comparecimento:** eleitoras e eleitores que foram habilitados(as) na urna e confirmaram o seu voto para ao menos um cargo. O total será o somatório da *habilitação biométrica*, *habilitação biográfica* e *habilitação sem biometria*.
12. **Eleição:** conjunto de cargos que possuem alguma associação e são disputados no mesmo conjunto de localidades. Os cargos de prefeito e vereador fazem parte da mesma eleição municipal, enquanto um plebiscito faz parte de outra eleição.



13. **Eleitoras/Eleitores aptos(as):** total de pessoas inscritas numa seção eleitoral habilitadas a votar. A quantidade será o somatório dos *originais da seção* com *temporários na seção*.
14. **Eleitoras/Eleitores faltosos(as):** votantes que não foram habilitados na urna.
15. **Eleitoras/Eleitores com transferência temporária:** sufragistas que não estiverem em seu domicílio eleitoral, no primeiro, no segundo ou em ambos os turnos, poderão votar em trânsito nas capitais e nos municípios com mais de 100 mil votantes. A configuração do processo eleitoral com várias eleições diferentes permite que eleitoras e eleitores que estão temporariamente transferidos(as) possam votar nos cargos que estão disponíveis.
16. **Fase da eleição:** distinção entre os conjuntos de dados do processo eleitoral, com a finalidade de separar a operação dos sistemas eleitorais entre os ambientes de produção e de homologação. A Justiça Eleitoral utiliza três fases, usando dados reais ou fictícios do eleitorado e das candidaturas, a saber: *oficial* – ambiente de produção, com dados reais; *simulado* – homologação e desenvolvimento, com dados fictícios; e *treinamento* – com dados fictícios, criados especificamente para que público votante, mesárias, mesários, escrutinadoras e escrutinadores aprendam a operar a urna eletrônica.
17. **Fechamento da urna:** momento em que a urna não mais aceita a coleta de votos.
18. **Habilitação biográfica:** em seções biométricas, corresponde ao total de votantes com biometria cadastrada cujas digitais não foram reconhecidas mas foram liberados para votar pelo(a) presidente da seção eleitoral com base no ano de nascimento da eleitora ou do eleitor.
19. **Habilitação biométrica:** em seções biométricas, corresponde ao total de eleitoras e de eleitores que foram liberados(as) para votar com o reconhecimento das respectivas biometrias.
20. **Habilitação sem biometria:** total de eleitoras e de eleitores sem biometria liberados(as) para votar pelo(a) presidente da seção eleitoral com base no ano de nascimento do(a) votante.
21. **Local de votação:** local escolhido pela eleitora ou pelo eleitor para votar, tal como um colégio ou uma faculdade, onde são distribuídas urnas eletrônicas para cada seção eleitoral.
22. **Origem do Boletim de Urna (BU):** o BU normalmente é gerado pelo Software de Votação (VOTA), porém, em casos de contingência, pode também ser gerado pelo Recuperador de Dados (RED) ou pelo Sistema de Apuração (SA).
23. **Originais da seção:** total de público votante que pode votar cuja seção de origem é a indicada no BU.
24. **Pleito:** todo o conjunto de dados e processos relacionados a um dos dias de votação, tais como o primeiro e o segundo turnos. Um pleito sempre está associado a um processo eleitoral. O resultado da votação na urna é sempre associado a um pleito.
25. **Processo eleitoral:** todo o conjunto de dados e processos relacionados a um período eleitoral, contemplando a definição do eleitorado, o registro de candidatas e de candidatos, a preparação das urnas e a totalização dos resultados. Uma vez definido o eleitorado, por exemplo, ele passa a ser válido para todo o processo eleitoral.
26. **Recuperador de Dados:** aplicativo da urna eletrônica utilizado, na junta eleitoral, sob autorização de uma juíza ou de um juiz eleitoral, para proceder à recuperação de dados de uma urna eletrônica que não foi encerrada corretamente.



27. **Seção biométrica:** seção eleitoral de uma localidade que já passou pelo cadastramento do eleitorado com a coleta de dados biométricos.
28. **Seção eleitoral:** ambiente no qual a eleitora e o eleitor devem votar. A uma seção eleitoral corresponde uma urna eletrônica. No momento de alistamento, a pessoa votante é inscrita numa seção eleitoral e somente nela ela poderá votar.
29. **Sistema de Apuração:** aplicativo da urna eletrônica utilizado na junta eleitoral, sob autorização de uma juíza ou de um juiz eleitoral, como meio complementar de apuração dos votos de uma seção eleitoral, nos casos em que houve votação por cédula de papel.
30. **Software de Votação:** aplicativo da urna eletrônica responsável pela habilitação da eleitora, do eleitor, da coleta de votos e da apuração na seção eleitoral.
31. **Temporários na seção:** total de público votante apto a votar transferido temporariamente para a seção indicada no BU (ver Eleitoras e Eleitores com Transferência Temporária).
32. **Tipo de eleição:** as eleições do tipo *legal* são aquelas ordinárias, que elegem candidatas e candidatos ao cargo de presidente, prefeito, vereador, deputado e senador, enquanto que as do tipo *comunitária* são eleições de entidades, tais como OAB, Confea etc.
33. **Totalização:** contabilização do resultado consolidado de todas as seções eleitorais.
34. **UE:** sigla de urna eletrônica.
35. **Voto de legenda:** para cargos proporcionais, é o voto destinado a um partido político.
36. **Voto em branco:** voto não destinado a uma candidata, a um candidato ou a um partido, registrado quando o eleitor pressiona a tecla BRANCO da urna.
37. **Voto nominal:** voto destinado a candidata, candidato ou resposta de consulta, cadastrado(a) na urna.
38. **Voto nulo:** voto correspondente à digitação de um número que não corresponde a nenhuma candidata, nenhum candidato, partido ou nenhuma resposta de consulta popular cadastrado(a) na urna.
39. **Zerésima:** documento emitido em cada seção eleitoral, indicando que não existe voto registrado. Este documento é emitido após o procedimento de inicialização da urna eletrônica, servindo para atestar que não há registro de voto para nenhuma candidata ou nenhum candidato.
40. **Zona eleitoral:** região geograficamente delimitada dentro de um estado, gerenciada pelo cartório eleitoral, que centraliza e coordena o público votante ali domiciliado. Pode ser composta por mais de um município ou por parte dele. Normalmente segue a divisão de comarcas da Justiça estadual.

#VOZ DA
DEMOCRACIA
ELEIÇÕES 2024



**Justiça
Eleitoral**
A Justiça da Democracia