Autenticação no NTP.br

Alexandre Y. Harano e Antonio M. Moreiras

Núcleo de Informação e Coordenação do Ponto BR – NIC.br

{harano,moreiras}@nic.br

`http://ntp.br/`

GTER 32 – São Paulo, 02 de dezembro de 2011.

Resumo

Apresentação de conceitos básicos relacionados ao NTP e ao protocolo de autenticação Autokey com o intuito de oferecer, em caráter experimental, a autenticação dos servidores NTP.br.

Tópicos

NTP

Sincronização de Tempo

NTP.br

Hora Legal Brasileira

Autenticação no NTP – Autokey

Validação de Mensagens NTP Assinadas

Network Time Protocol (NTP)

- Especificação do NTPv4: **RFC 5905**.
- NTP denota por:
  1. Software (*daemon*)
  2. Protocolo
  3. Algoritmos de seleção de fontes e alteração do relógio local
- Serviço de sincronização de tempo via rede dividido em níveis hierárquicos denominados *estratos*.
- Transporte por UDP via porta 123.

Tópicos

NTP

Sincronização de Tempo

NTP.br

Hora Legal Brasileira

Autenticação no NTP – Autokey

Validação de Mensagens NTP Assinadas

Acordo: Observatório Nacional e NIC.br

Observatório Nacional (ON)

- Geração, conservação e disseminação da Hora Legal Brasileira, através de relógios atômicos.
- Contribui para a escala de Tempo Atômico Internacional (TAI), mantida pelo Bureau International des Poids et Mesures (BIPM), localizado na França.

NIC.br

- Distribuição gratuita da Hora Legal Brasileira via internet, através do protocolo NTP.

Resolução CGI.br sobre o uso do NTP

Resolução ***CGI.br/RES/2008/009/P***

"Recomendação para a Sincronização de relógios via NTP"

Finalidade

- Correto funcionamento de sistemas e redes.
- Apoio a processos de detecção de incidentes de segurança e seu tratamento adequado, permitindo a correlação de eventos.
- Documentação e preservação de evidências que possam vir a ser utilizadas em investigações de crimes de informática.

Resolução CGI.br sobre o uso do NTP

Recomendações

- Sincronizar a fontes de tempo confiáveis de forma continuada todos os dispositivos de rede, servidores e estações de trabalho conectados à Internet no Brasil com a Horal Legal Brasileira.
- Estabelecer procedimentos de ajuste do tempo ao fuso horário local e ao horário de verão, quando necessários.
- Gerar registro de eventos pertinentes, de forma a manter informações inequívocas sobre o fuso horário em que se deu um evento.
- Utilizar, preferencialmente, o protocolo NTP e os servidores de tempo implantados pelo NIC.br, conforme instruções e recomendações contidas em `http://ntp.br/`

Localização dos Servidores NTP.br

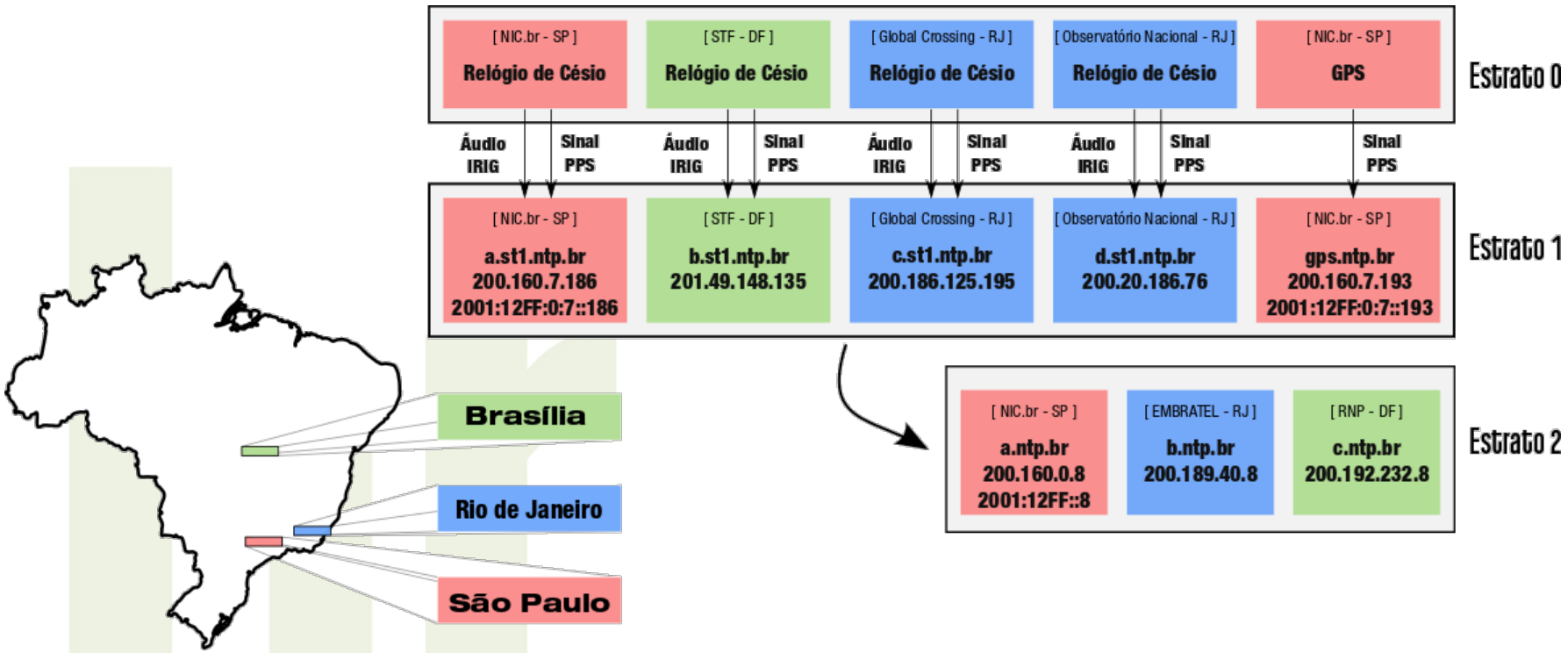


Figura: Estrutura hierárquica dos servidores NTP.br.

Tópicos

NTP

Sincronização de Tempo

NTP.br

Hora Legal Brasileira

Autenticação no NTP – Autokey

Validação de Mensagens NTP Assinadas

O que é Autokey?

- Especificação do Autokey para NTPv4: **RFC 5906**.
- Baseado na Infraestrutura de Chaves Públicas (ICP).
- Mecanismo de segurança que considera a vida útil da informação de tempo.
- Documentação vincula o uso da biblioteca OpenSSL.

Por que usar o Autokey?

- Garante a autenticidade das fontes de tempo desde a raiz do grupo seguro NTP (trilha de certificação).
- Minimiza ataques *man-in-the-middle* (quando utilizado com esquemas de identificação).
- Filtra pela validade das mensagens antes de verificar assinatura.
- Não há troca de mídia criptográfica durante seu uso (chaves de *host*, assinatura e identidade).
- Criptoanálise das mídias não é viável para sua vida útil.

Usando Autokey com Servidores NTP.br

1. Obtenção dos parâmetros através de solicitação para

   `ntp@nic.br`

2. Alteração do `ntp.conf`.

ntp.conf

- Sem Autokey

```
server a.ntp.br iburst
server b.ntp.br iburst
server c.ntp.br iburst
```

- Com Autokey

```
server a.ntp.br iburst autokey
server b.ntp.br iburst autokey
server c.ntp.br iburst autokey

crypto pw ASENHA digest SHA1
keysdir /etc/ntp
```

Usando Autokey com Servidores NTP.br

3. Compilação da versão estável mais recente da implementação de referência (ntp 4.2.6p4).
4. Geração de chaves de *host* e assinatura conforme os parâmetros.

```
ntp-keygen -H -S DSA -c DSA-SHA1 -p ASENHA
```

5. Periodicamente (e.g. `cron`) regerar a chave de *host*, através de

```
ntp-keygen -q ASENHA
```

A recomendação é de atualização mensal.

Grupo Seguro NTP

Certificado autoassinado

Cada *host* deve possuir um certificado X.509 autoassinado, usualmente com validade de 1 ano.

Autoridade confiável (*trusted authority*)

Responsável pela gerência dos parâmetros do grupo. Pode ser uma máquina externa à rede.

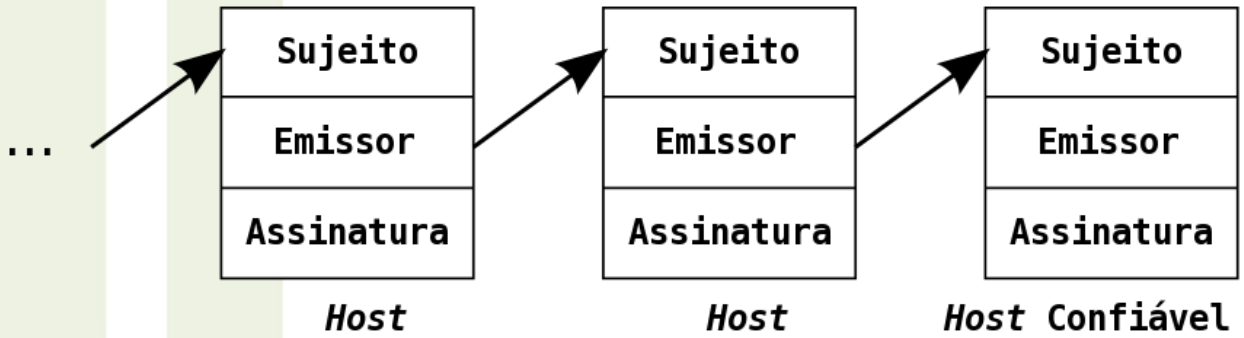
Hosts confiáveis (*trusted hosts*)

Possuem o menor estrato da rede e são os únicos *hosts* cujos certificados são marcados como confiáveis.

Grupo Seguro NTP

Trilha de certificação (*proventic trail*)

- *Hosts* confiáveis possuem como trilha de certificação seus próprios certificados autoassinados.
- Cliente solicita assinatura de seu certificado a seus servidores, além de suas trilhas de certificação. Todos os certificados da trilha do cliente, servidores intermediários até a raiz são armazenados em cache.



Grupo Seguro NTP

```
cert="M.local a.ntp.br 0x4", until=201211302013,
cert="M.local c.ntp.br 0x4", until=201211302012,
cert="M.local b.ntp.br 0x4", until=201211302012,
cert="c.ntp.br b.st1.ntp.br 0x6", until=201211061531,
cert="b.st1.ntp.br b.st1.ntp.br 0x5", until=201210310730,
cert="b.ntp.br b.st1.ntp.br 0x6", until=201211061515,
cert="a.ntp.br b.st1.ntp.br 0x6", until=201211061511,
cert="M.local M.local 0x0", until=201211300142
```

Figura: Exemplo de saída da consulta `ntpq -c "rv 0 cert"` com 3 servidores: `a.ntp.br`, `b.ntp.br` e `c.ntp.br`.

Grupo Seguro NTP

Fonte verificada (*proventic source*)

Servidores NTP que já possuem trilha de certificação do grupo em questão.

Sincronização

Um cliente está sincronizado a uma fonte verificada quando uma ou mais associações verificadas pertencentes ao grupo são selecionadas pelos algoritmos de escolha de relógios.

Grupo Seguro NTP

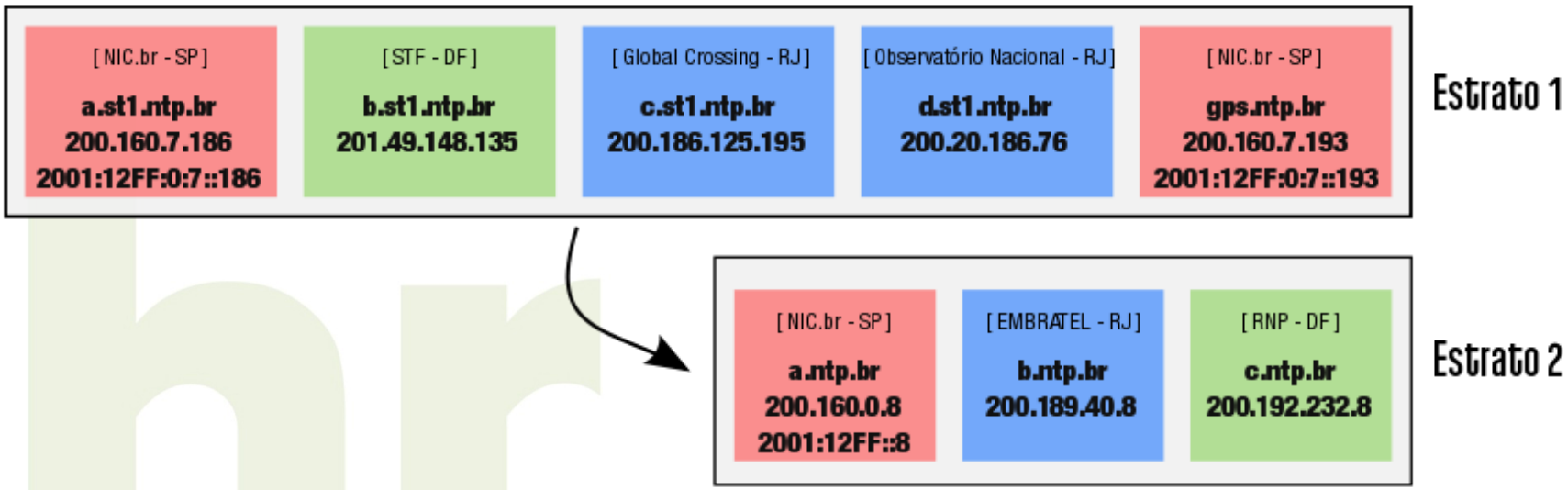


Figura: No NTP.br, cada servidor estrato 1 possui um grupo seguro equivalente.

Como opera o Autokey?

- Possui 3 modos para a operação do protocolo:
  1. Cliente/servidor.
  2. Simétrico.
  3. *Broadcast*.
- Sequência de solicitações/respostas (*dança*).

Dança Cliente/Servidor

1. Troca de Parâmetros.
2. Recuperação de Certificados.
3. Identificação.
4. Envio de *Cookie*.
5. Espera por Sincronização.
6. Assinatura.
7. Envio de Segundos Intercalados.

Dança Cliente/Servidor

1. Troca de Parâmetros.
2. Recuperação de Certificados.
3. Identificação.
4. Envio de *Cookie*.
5. Espera por Sincronização.
6. Assinatura.
7. Envio de Segundos Intercalados.

Parâmetros

Cliente indica os esquemas de criptografia e de identificação que poderão ser utilizados conforme disponibilidade do servidor.

Dança Cliente/Servidor

1. Troca de Parâmetros.
2. Recuperação de Certificados.
3. Identificação.
4. Envio de *Cookie*.
5. Espera por Sincronização.
6. Assinatura.
7. Envio de Segundos Intercalados.

Certificados

Aquisição de trilha de certificação. Cliente entra em loop, no quesito autenticação, até obter toda a trilha.

Dança Cliente/Servidor

1. Troca de Parâmetros.
2. Recuperação de Certificados.
3. Identificação.
4. Envio de *Cookie*.
5. Espera por Sincronização.
6. Assinatura.
7. Envio de Segundos Intercalados.

Identidade

A identidade é verificada através de um mecanismo seguro de identificação, como *IFF*, *GQ* ou *MV* (serão abordados posteriormente).

Dança Cliente/Servidor

1. Troca de Parâmetros.
2. Recuperação de Certificados.
3. Identificação.
4. Envio de *Cookie*.
5. Espera por Sincronização.
6. Assinatura.
7. Envio de Segundos Intercalados.

Cookie

Cliente envia sua chave pública e o servidor devolve um *cookie* criptografado com essa chave. Esse *cookie* é usado para o cálculo da lista de chaves (abordado posteriormente).

Dança Cliente/Servidor

1. Troca de Parâmetros.
2. Recuperação de Certificados.
3. Identificação.
4. Envio de *Cookie*.
5. Espera por Sincronização.
6. Assinatura.
7. Envio de Segundos Intercalados.

Sincronização

Essa etapa é validada quando o cliente escolhe o servidor em questão como uma das referências no algoritmo de escolha de relógios.

Dança Cliente/Servidor

1. Troca de Parâmetros.
2. Recuperação de Certificados.
3. Identificação.
4. Envio de *Cookie*.
5. Espera por Sincronização.
6. Assinatura.
7. Envio de Segundos Intercalados.

Assinatura

Servidor cria um novo certificado com base no certificado apresentado pelo cliente, assinando-o e o envia ao cliente. Esse novo certificado é utilizado para assinar os certificados de seus possíveis clientes.

Dança Cliente/Servidor

1. Troca de Parâmetros.
2. Recuperação de Certificados.
3. Identificação.
4. Envio de *Cookie*.
5. Espera por Sincronização.
6. Assinatura.
7. Envio de Segundos Intercalados.

Segundos Intercalados (*Leapseconds*)

Determinado pelo *International Earth Rotation and Reference Systems Service* (*IERS*). Ajusta o UTC conforme alteração de parâmetros físicos.

Esquema de Identificação

- *Schnorr – Identify Friendly or Foe* (*IFF*).
- *Guillou-Quisquater* (*GQ*).
- *Mu-Varadharajan* (*MV*).

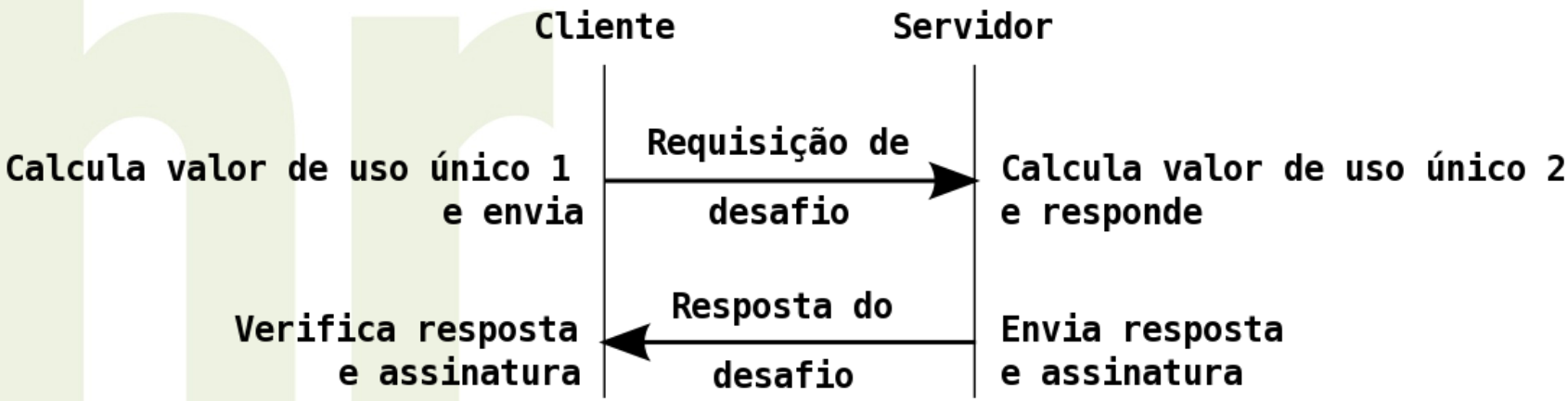


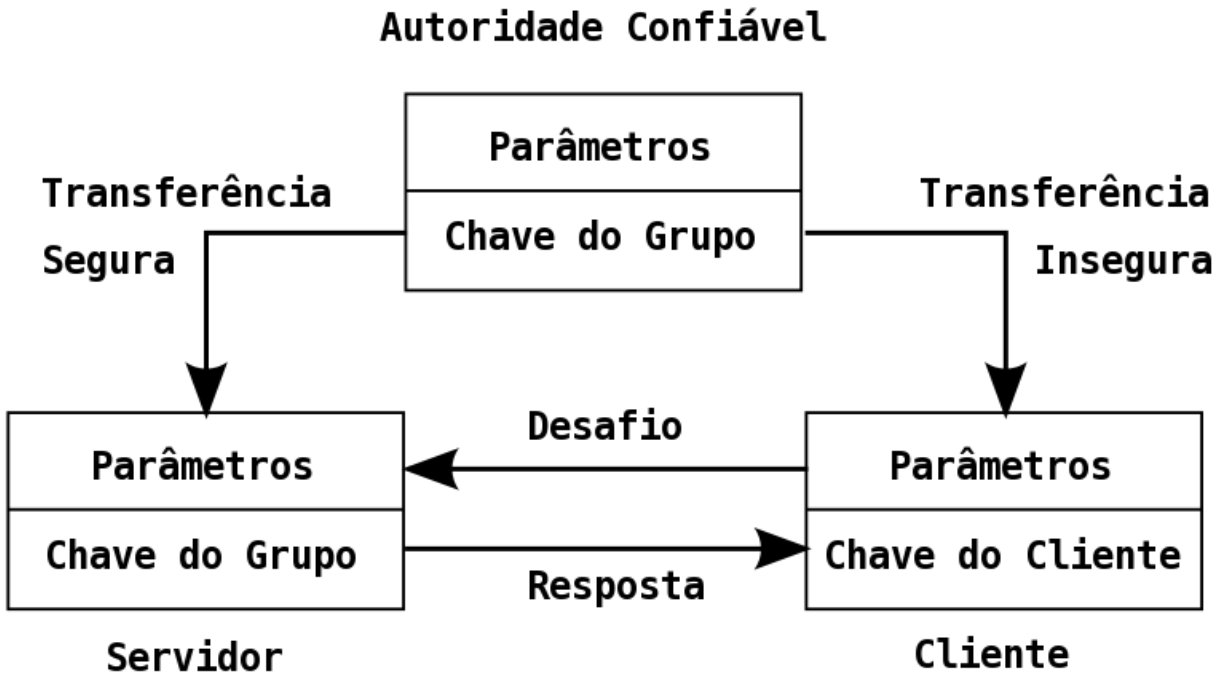
Figura: Troca de Identidades.

Esquema de Identificação

IFF

Princípios matemáticos similares ao DSA.

- *Schnorr – Identify Friendly or Foe* (*IFF*).
- *Guillou-Quisquater* (*GQ*).
- *Mu-Varadharajan* (*MV*).

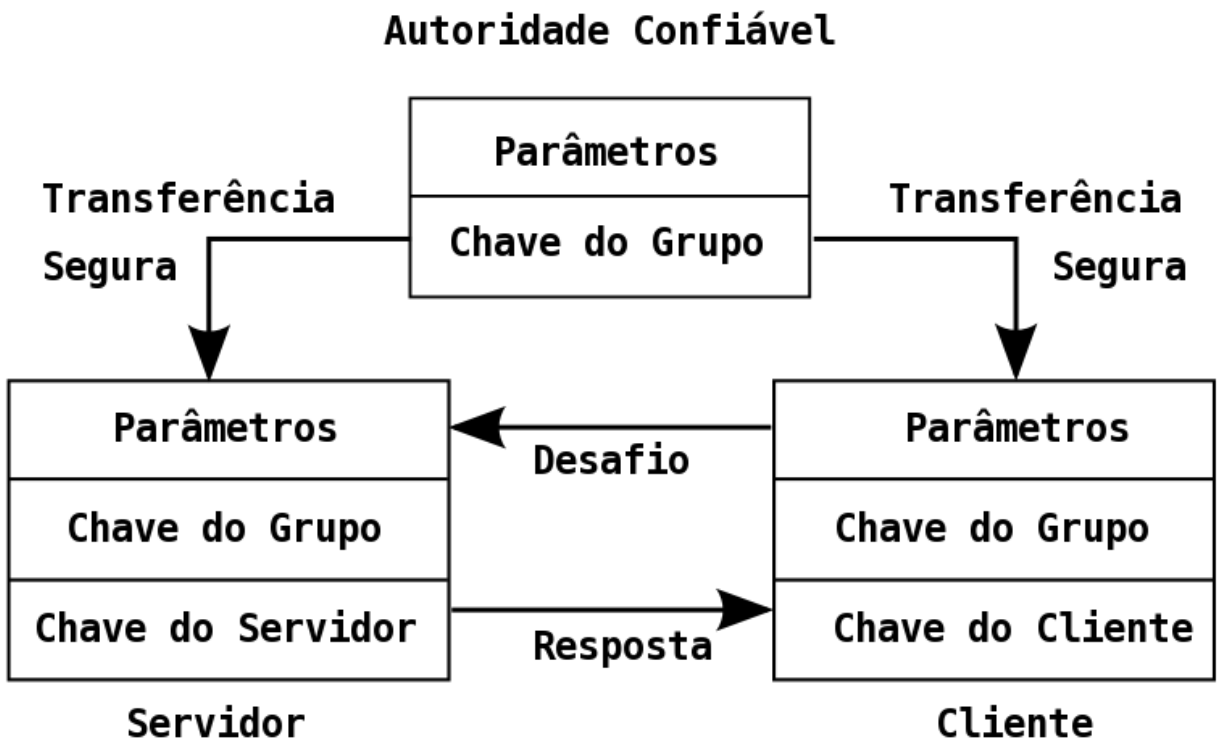


Esquema de Identificação

- *Schnorr – Identify Friendly or Foe* (*IFF*).
- *Guillou-Quisquater* (*GQ*).
- *Mu-Varadharajan* (*MV*).

GQ

Princípios matemáticos similares ao RSA.

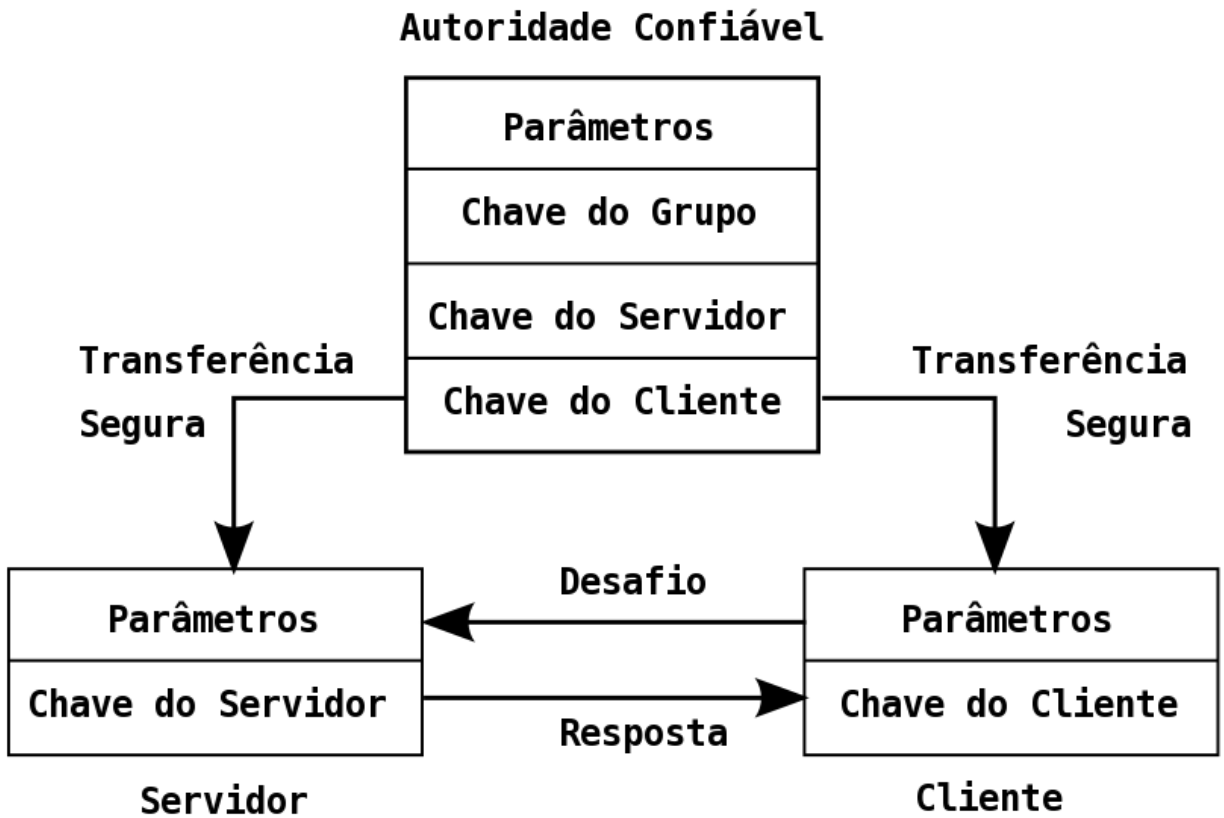


Esquema de Identificação

- *Schnorr – Identify Friendly or Foe* (*IFF*).
- *Guillou-Quisquater* (*GQ*).
- *Mu-Varadharajan* (*MV*).

MV

Parâmetros equivalente ao DSA.



Exemplo de Arquivo de Parâmetros IFF

```
# ntpkey_iffpar_gps.ntp.br.3526663276
# Mon Oct  3 17:41:16 2011

-----BEGIN DSA PRIVATE KEY-----
MIHlAgEAAkEAt3Fk/E1JTbvqbhJmGe+S8H7rS3fkSeWaGIVPbyR6GEmqhA/219UP
bSuLqhthXtbOFbdbt1OH6aKsxd1QYoJtjQIVAJ14xYUTjynQVfV3egHUoDeZCz6f
AkEAlVadPaZHzdhL1rMf/3xOS+JDXYehNcP3XiM4xDZJReoKqUisY8Xo8O1R5wRB
w1T68DOU21w4+3vQi29RSjcxiAJAU107EDrPaLcLnvcIfkGZvLd7QKTEGUs25f7M
4dvPziRmvl9jvNTEwug15PaZPjlntFNN1iB18Z9d0f8rjk4/BAIBAQ==
-----END DSA PRIVATE KEY-----
```

Criptografia Autokey

Figura: Estrutura da chave *autokey*.

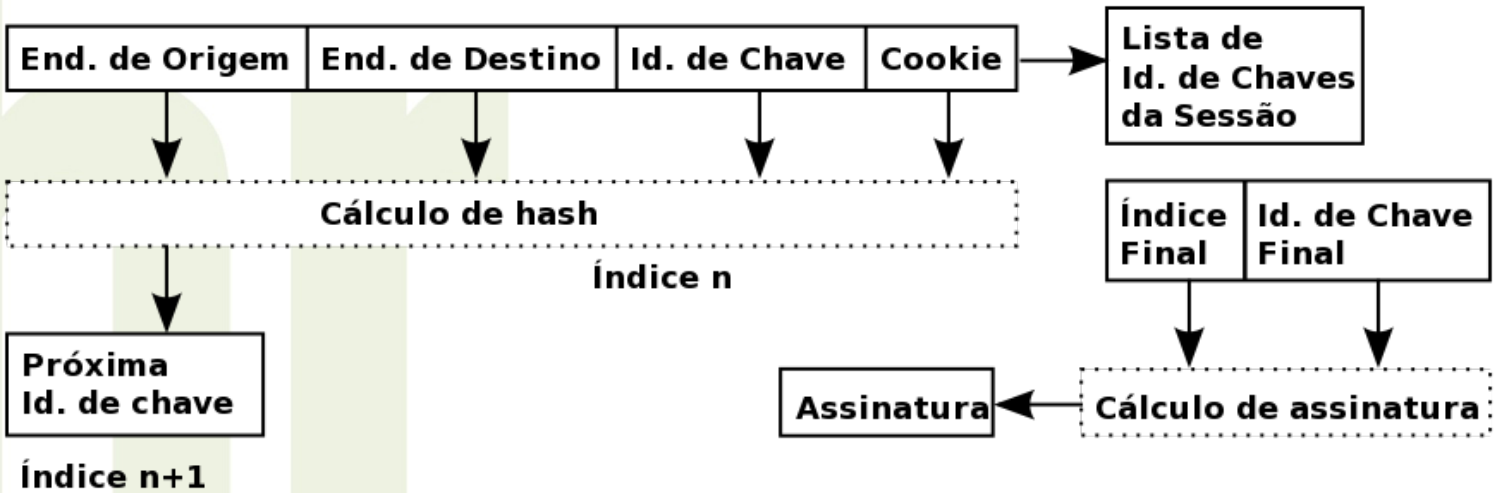


Figura: Geração de lista de *autokeys*.

Criptografia Autokey

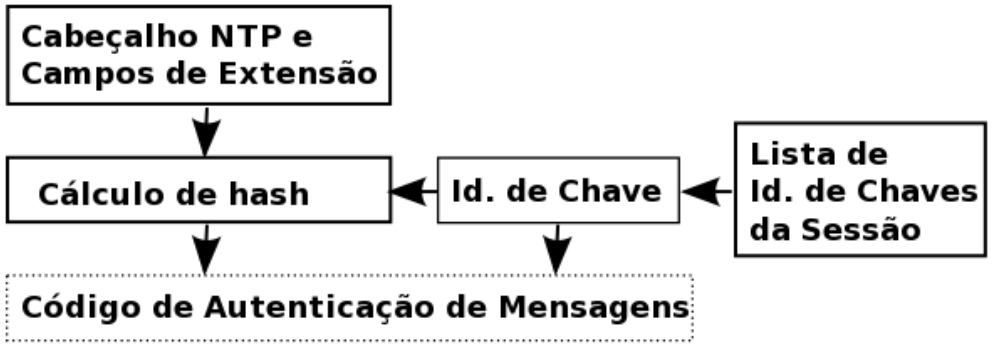


Figura: Transmissão de Mensagens.

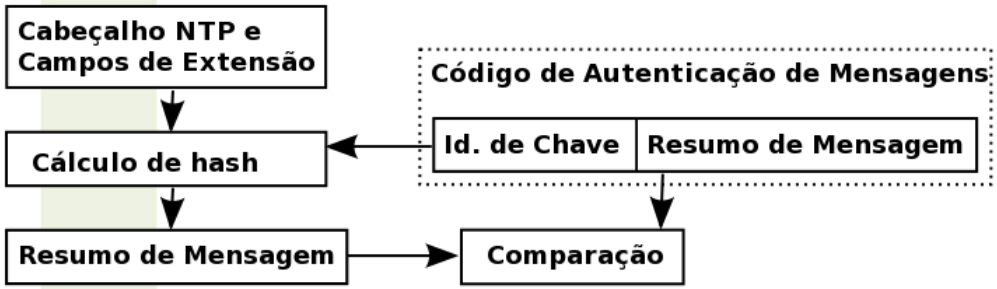


Figura: Autenticação de Mensagens.

Resumo

Autokey

Mecanismo de validação de mensagens com listas de chaves de uso único geradas de modo pseudo-aleatório.

Grupo Seguro NTP

Estrutura hierárquica nivelada por estratos envolvendo uma autoridade confiável e *hosts* confiáveis.

Esquema de Identificação

Modelo de validação de servidores pertencentes a um grupo, através de requisições desafio/resposta.

NTP.br

Todos os servidores NTP.br disponibilizam a autenticação em caráter experimental. Os parâmetros podem ser solicitados para `ntp@nic.br`.

Referência

David L. Mills.
Computer Network Time Synchronization: the Network Time Protocol on Earth and in Space, Second Edition.
CRC Press 2011, 466 pp.

RFC 5905 *Network Time Protocol Version 4: Protocol and Algorithms Specification*
`http://tools.ietf.org/html/rfc5905`

RFC 5906 *Network Time Protocol Version 4: Autokey Specification*
`http://tools.ietf.org/html/rfc5906`

NTP *ntp.org: Home of the Network Time Protocol*
`http://www.ntp.org/`

Support *The NTP Public Services Project*
`http://support.ntp.org/`

Obrigado!

Solicitação de beta testers para uso do Autokey

ntp@nic.br

`http://ntp.br/`

cgi.br nic.br ntp.br

ON
OBSERVATÓRIO NACIONAL