Secure Integration

Christian Grothoff

Berner Fachhochschule

20.3.2026

Learning Objectives

How can we securely integrate services?

Terminology

How to register a URI scheme?

Example: RFC 8905

Example: LSD 0006

System Security

Part I: System Security

Hardware

General notions:

- Hardware is the foundation for secure architecture: memory management, isolation, etc.
- Platforms with disabled Intel ME & disabled remote administration are safer.
- Platforms using uncommon CPU archtectures (Power7, Sparc) are safer.
- VMs are not a security mechanism. Side-channel attacks abound. Avoid running any software in a virtual machine “for security”.

Operating system

General notions:

- It should be safe to run different reasonably secure components (such as Nginx and Postgres) on the same physical hardware (under different UIDs/GIDs). You may want to separate them onto different physical machines during scale-out, but not necessarily for “basic” security.
- Limiting and auditing system administrator access will be crucial.
- Recommend to **not** use any anti-virus: more of a liability than an asset.
- Recommend using a well-supported GNU/Linux operating system (such as Debian or Ubuntu or Nix).

Secure Integration

Part II: Secure Integration

Integration: Problem Statement

Isolation is a key paradigm in security:

- processes (address spaces!)
- users (quotas, access rights)
- departments (accounting, controlling, revision)
- organizations (auditors)

Integration: Problem Statement

Isolation is a key paradigm in security:

- processes (address spaces!)
- users (quotas, access rights)
- departments (accounting, controlling, revision)
- organizations (auditors)

How to ensure good user experience across application boundaries?

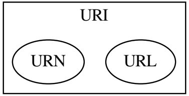
Solution domains

- Fax

Solution domains

- Fax
- Inter-process communication (UNIX Domain Sockets, Shared Memory, Networking)
- Intents (Android-only!)
- **Deep links**

Addressing



URI Uniform Resource Identifier

URL Uniform Resource Locator — object identification tied to location

URN Uniform Resource Name — namespace independent of location

Structure of a URI

URI = scheme “:” hierarchical-part [“?” query] [“#” fragment]

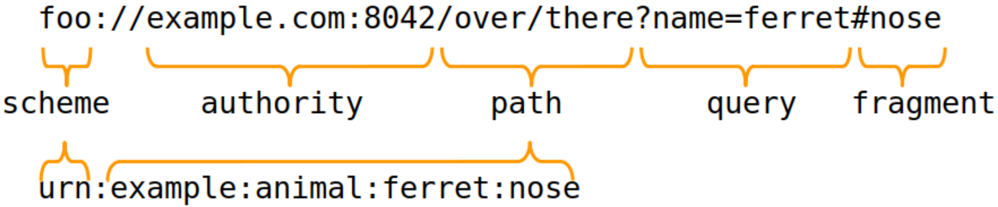
scheme Defines the method of identification

hierarchical part Hierarchical access path of the URI

query Search function

fragment access to a part of the document

URI/URN examples



foo://example.com:8042/over/there?name=ferret#nose

scheme authority path query fragment

urn:example:animal:ferret:nose

The Internet Assigned Numbers Authority (IANA)

- Responsible for unique assignment of parameters and numbers in Internet protocols
- Operates the DNS root zone
- Performs the administrative work *on behalf of* ICANN and IETF
- Web site: `https://iana.org/`
- Used to be just Jon Postel

Common URI scheme

ftp	File Transfer Protocol [1]
http	Hyper Text Transfer Protocol [2]
https	HTTP Secure [7]
mailto	Electronic mail address [4]
file	Host-specific file names [1]
imap	Internet Message Access Protocol [5]
pop	Post Office Protocol v3 [3]
ldap	Lightweight Directory Access Protocol [8]
urn	Uniform Resource Names[1] [6]

Except from `http://www.iana.org/assignments/uri-schemes`.

[1] `http://www.iana.org/assignments/urn-namespaces`

URI examples

```
http://prof.hti.bfh.ch/index.php?id=1403&L=2#howto
http://[2001:620:500:ff80::80]/owncloud

ftp://ftp.rfc-editor.org/in-notes/rfc3986.txt
ftp://user:geheim@ftp.bfh.ch/

file:///C:/WINDOWS/system32/drivers/etc/services
mailto:firstname.lastname@bfh.ch

urn:ietf:rfc:3986
urn:ISBN:1-56592-862-8
```

Security Considerations

- Link hijacking: malicious or competing apps can register for your scheme
- Data interception: links with sensitive data may be transmitted by users over insecure channels
- Access control bypass: ensure checking access when handling links
- Insecure parameter handling: strings are the source of all eval

How to register a URI scheme? [9]

There are *permanent* and *provisional* registrations. Always start with *provisional*, but largely follow *permanent* guidelines:

1. Write and publish citable specification (ideally, RFC-style) explaining the use-case, syntax, semantics and security considerations
2. Follow syntactic requirements and ensure name is not taken
3. Send a registration request to `uri-review@ietf.org` and possibly other relevant lists for discussion.
4. Respond to comments, address in specification where reasonable (wait a few weeks for discussion to conclude).
5. Submit updated registration request to *iana@iana.org* with pointer to the discussion.

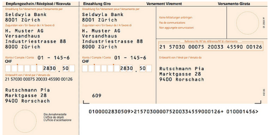
You can always “upgrade” to *permanent* status later!

RFC 8905: payto: Uniform Identifiers for Payments and Accounts

Like mailto:, but for bank accounts instead of email accounts!

```
payto://<PAYMENT-METHOD>/<ACCOUNT-NR>
  ?subject=InvoiceNr42
  &amount=EUR:12.50
```

Default action: Open app to review and confirm payment.



Empfangsschein / Récépissé / Ricevuta

Einzahlung für / Versement pour / Versamento per

Seldwyla Bank
8001 Zürich

Zugunsten von / En faveur de / A favore di

H. Muster AG
Versandhaus
Industriestrasse 88
8000 Zürich

Konto / Compte / Conto 01 - 145-6

CHF 2830 . 50

Einbezahlt von / Versé par / Versato da

21 57030 00075 20033 45590 00126

Rutschmann Pia
Marktgasse 28
9400 Rorschach

Die Annahmestelle
L'office de dépôt
L'ufficio d'accettazione

Einzahlung Giro **Versement Virement** **Versamento Girata**

Einzahlung für / Versement pour / Versamento per

Seldwyla Bank
8001 Zürich

Zugunsten von / En faveur de / A favore di

H. Muster AG
Versandhaus
Industriestrasse 88
8000 Zürich

Konto / Compte / Conto 01 - 145-6

CHF 2830 . 50

609

Keine Mitteilungen anbringen
Pas de communications
Non aggiungete comunicazioni

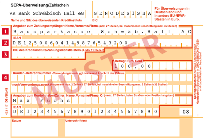
Referenz-Nr. / N° de référence / N° di riferimento

21 57030 00075 20033 45590 00126

Einbezahlt von / Versé par / Versato da

Rutschmann Pia
Marktgasse 28
9400 Rorschach

0100002830509>215703000075200334559000126+ 010001456>



SEPA-Überweisung/Zahlschein

VR Bank Schwäbisch Hall eG

Name und Sitz des überweisenden Kreditinstituts

BIC: GENODES1SHA

Für Überweisungen in Deutschland und in andere EU-/EWR-Staaten in Euro.

1 Angaben zum Zahlungsempfänger: Name, Vorname/Firma (max. 27 Stellen, bei maschineller Beschriftung max. 35 Stellen)

Bausparkasse Schwäb.Hall AG

2 IBAN

DE12500604149876543200

3 BIC des Kreditinstituts/Zahlungsdienstleisters (8 oder 11 Stellen)

Betrag: Euro, Cent

100,00

4 Kunden-Referenznummer - Verwendungszweck, ggf. Name und Anschrift des Zahlers

noch Verwendungszweck (insgesamt max. 2 Zeilen à 27 Stellen, bei maschineller Beschriftung max. 2 Zeilen à 35 Stellen)

Angaben zum Kontoinhaber/Zahler: Name, Vorname/Firma, Ort (max. 27 Stellen, keine Straßen- oder Postfachangaben)

Max Fuchs

IBAN

DE12345678901234567890

08

Datum

Unterschrift(en)

Schreibmaschine: normale Schreibweise!
Handschrift: Blockschrift in GROSSBUCHSTABEN und dabei Kästchen beachten!

423 417 DG VERLAG

MUSTER

Benefits of `payto://`

- Standardized way to represent financial resources (bank account, bitcoin wallet) and payments to them
- Useful on the client-side on the Web and for FinTech backend applications
- Payment methods (such as IBAN, ACH, Bitcoin) are registered with GANA [2]

[2] https://gana.gnunet.org/

Security Considerations for `payto://`

- Interactive applications handling the ’payto’ URI scheme MUST NOT initiate any financial transactions without confirmation from the user and MUST take measures to prevent clickjacking.
- Unless a ’payto’ URI is received over a trusted, authenticated channel, a user might not be able to identify the target of a payment. A payment target type SHOULD NOT use human-readable names in combination with unicode in the target account specification.
- The authentication/authorization mechanisms used to process a payment encoded in a ’payto’ URI are handled by the application and are not in scope of this document.
- Payment target types SHOULD NOT include personally identifying information about the sender of a payment that is not essential to conduct a payment.

LSD 0006: `taler:` wallet triggers

https://lsd.gnunet.org/lsd0006/

Syntax:

```
taler-URI = ("taler://" / "TALER://" / "taler+http://"
               / "TALER+HTTP://" )
            action path-abempty [ "?" opts ]
action = ALPHA *( ALPHA / DIGIT / "-" / "." )
opts = opt *( "&" opt )
opt = opt-name "=" opt-value
opt-name = ALPHA *( ALPHA / DIGIT / "-" / "." / ":" )
opt-value = *pchar
```

Example:

```
taler://pay-push/exchange.taler.grothoff.org/D83MG3W7WKVH3C9...
```

taler:// actions

withdraw	bank-initiated withdrawal
pay	merchant-initiated payment
refund	merchant-initiated refund
pay-push	P2P payment
pay-pull	P2P invoice
pay-template	merchant offline payment
restore	restore from backup
withdraw-exchange	wallet-initiated withdrawal

References I

T. Berners-Lee, L. Masinter, and M. McCahill.
Uniform Resource Locators (URL).
RFC 1738 (Proposed Standard), December 1994.
Obsoleted by RFCs 4248, 4266, updated by RFCs 1808, 2368, 2396, 3986, 6196, 6270, 8089.

References II

- R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee.
  Hypertext Transfer Protocol – HTTP/1.1.
  RFC 2616 (Draft Standard), June 1999.
  Obsoleted by RFCs 7230, 7231, 7232, 7233, 7234, 7235, updated by RFCs 2817, 5785, 6266, 6585.

- R. Gellens.
  POP URL Scheme.
  RFC 2384 (Proposed Standard), August 1998.

References III

- P. Hoffman, L. Masinter, and J. Zawinski.
  The mailto URL scheme.
  RFC 2368 (Proposed Standard), July 1998.
  Obsoleted by RFC 6068.

- A. Melnikov and C. Newman.
  IMAP URL Scheme.
  RFC 5092 (Proposed Standard), November 2007.
  Updated by RFC 5593.

References IV

- R. Moats.
  URN Syntax.
  RFC 2141 (Proposed Standard), May 1997.
  Obsoleted by RFC 8141.

- E. Rescorla.
  HTTP Over TLS.
  RFC 2818 (Informational), May 2000.
  Updated by RFCs 5785, 7230.

References V

- M. Smith and T. Howes.
  Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator.
  RFC 4516 (Proposed Standard), June 2006.

- D. Thaler, T. Hansen, and T. Hardie.
  Guidelines and Registration Procedures for URI Schemes.
  RFC 7595 (Best Current Practice), June 2015.

Acknowledgements

Co-funded by the European Union (Project 101135475).

**Co-funded by
the European Union**

Co-funded by SERI (HEU-Projekt 101135475-TALER).

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union.

Neither the European Union nor the granting authority can be held responsible for them.