



Payment Card Industry **3-D Secure (PCI 3DS)**

Attestation of Compliance

For use with PCI 3DS Core Security Standard v1.0

Revision 1.0

December 2017

Section 1: 3DS Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the 3DS entity's assessment with the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (PCI 3DS Core Security Standard). Complete all sections. The 3DS entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the payment brands for PCI 3DS reporting and submission procedures.

Part 1. 3DS Entity and 3DS Assessor Information					
Part 1a. 3DS Entity Organization Information					
Company Name:	N&TS GROUP Networks & Transactional Systems Group S.p.A.	DBA (doing business as):	N/A		
Contact Name:	Loredana Febelli	Title:	Compliance Manager		
Telephone:	+39 02 8227651	E-mail:	l.febelli@netsgroup.com		
Business Address:	Strada 4, palazzo A5 20057 Assago (MI) Italy	City:	Milan		
State/Province:	N/A	Country:	Italy	Zip:	20057
URL:	www.netsgroup.com				
Part 1b. 3DS Assessor Company Information					
Company Name:	Dot.Bit d.o.o.				
Lead 3DS Assessor Contact Name:	Branimir Pacar	Title:	Principal Consultant		
Telephone:	+385992265696	E-mail:	branimir.pacar@dotbit.eu		
Business Address:	Stubicka 48a	City:	Zagreb		
State/Province:	N/A	Country:	Croatia	Zip:	10110
URL:	https://dotbit.eu				
Part 2. Executive Summary					
Part 2a. 3DS Functions					
Identify the 3DS Function(s) covered by this 3DS assessment (Check all that apply)	Details of EMVCo Letter of Approval (LOA):				
<input checked="" type="checkbox"/> 3DS Server (3DSS)	LOA reference number: 3DS_LOA_SER_NTGN_020200_00525_31Jan22 Date of LOA issued by EMVCo: January 31, 2022 Name of product LOA issued for: IGFS 3DS SERVER				
<input checked="" type="checkbox"/> Access Control Server (ACS)	LOA reference number: 3DS_LOA_ACS_NTGN_020200_00526_31Jan22 Date of LOA issued by EMVCo: January 31, 2022 Name of product LOA issued for: ACFS 3DS ACS				
<input type="checkbox"/> Directory Server (DS)	LOA reference number: Date of LOA issued by EMVCo: Name of product LOA issued for:				

Other (As defined by a payment brand)

Note: If your organization performs 3DS functions that are not covered by this assessment, consult the applicable payment brand about validation for the other functions.

Part 2b. Description of 3DS Business

How and in what capacity does your business provide/manage 3DS functions?

N&TS Group Networks & Transactional Systems Group S.p.A. (N&TS GROUP or N&TS hereafter) is an Italian Company which was established in 1995 to provide technology services to multinational retailers and financial services organizations. N&TS GROUP serves banks and acquirers to facilitate the processing of credit card transactions. The headquarter office is located in Assago (Milan), Italy.

N&TS GROUP provides several types of services. They function as a gateway for those who process face-to-face transactions through POS terminals.

As payments enter N&TS GROUP's network they are processed through the PA-DSS validated applications (FTFS and IGFS) on their Terminal Management servers where credit card information (encrypted PAN) is stored for a short time until it is sent to the acquirer as batch files for settlement. Customers terminate MPLS connections at the N&TS GROUP's firewall where specific ports are opened allowing transactions to be processed directly through N&TS GROUP's Terminal Manager. N&TS GROUP also provides a website form for e-commerce payments, and processes transactions when customers pay.

N&TS GROUP stores cardholder data (encrypted PAN) for 6-24 months depending on the contract with the customer for chargeback requests. N&TS GROUP also provides a protocol conversion service, ACFS, that acts as a gateway allowing customers to use the N&TS GROUP's Terminal Manager to convert transactions to other ISO formats allowing them to process payments through a variety of acquirers.

Furthermore, N&TS GROUP provides a MOTO channel, by which processes transactions when customers provide the data via a batch file PGP enciphered (email channel) or sending data to the moto server through the HTTPS protocol (telephone channel). Then, the Payment Gateway (IGFS) sends the authorization request by a protocol that depends on the specific acquirer. Upon completion, the transactional data (which includes encrypted PAN) is stored in the database. Cardholder data is encrypted according to the key management techniques provided by GRFS. CVV2 is never stored. 3DS authentication data is directly entered in forms published by the issuer. The response is made available to the merchant to inform them about the payment status via a batch file PGP encrypted.

Part 2c. Locations

List types of facilities (for example, corporate offices, data centers) and a summary of locations covered by the PCI 3DS assessment.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
<i>Example: Data Center</i>	3	<i>Boston, MA, USA</i>
Data Center	1	Ashburn, USA
Data Center	1	Secaucus, USA
Data Center	1	Frankfurt, Germany
Data Center	1	Basiglio, Italy
Corporate Office	1	Milan, Italy

Part 2d.

Not used for this AOC

Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

- *Connections into and out of the 3DS environment (3DE).*
- *Critical system components within the 3DE, such as 3DS servers, databases, web servers, etc., and any other necessary 3DS components, as applicable.*

The following services have been included into the scope of this assessment:

- 3D Secure ACS Provider
- 3D Secure 3DSS Provider

3DS ACS and 3DSS services are provided by a dedicated 3DS environment, which is logically segmented from the rest of PCI DSS Cardholder Data Environment (CDE). All connections to and from 3DE were included into the scope of assessment. The following 3DE components were included:

- ACS/3DSS database servers
- ACS/3DSS application servers
- ACS/3DSS web servers providing API access
- Network devices (firewalls, routers, switches)

Servers performing security functions like access control, IDS, FIM, centralized log management, NTP.

Does your business use network segmentation to affect the scope of your 3DS environment?

Yes No

Part 2f. Third-Party Service Providers

Does your company share 3DS data with any third-party service providers (for example, payment processors, gateways)? Yes No

Does your company rely on any third party for any PCI 3DS requirements, or for support or maintenance of the 3DS environment? Yes No

If Yes:

Name of service provider:	Description of services provided:
Equinix	Data center provider

Part 2g. Summary of requirements tested to the PCI 3DS Security Standard

Did the 3DS entity leverage a PCI DSS assessment to meet the PCI 3DS Part 1: Baseline Security Requirements? Yes No

Identify the appropriate assessment result for each high-level PCI 3DS requirement. Complete the table as follows:

- *If the results of a PCI DSS assessment have been verified as meeting all the PCI 3DS Part 1 Requirements:*
 - Select “In Place per PCI DSS” for the 3DS Part 1 Requirements.
 - Select the appropriate finding for each PCI 3DS Part 2 Requirement.
- *If a PCI DSS assessment is not being leveraged to meet all the PCI 3DS Part 1 Requirements:*
 - Select the appropriate finding for each 3DS Part 1 and Part 2 Requirement.

When determining the appropriate finding for each high-level 3DS requirement, the following principles apply:

1. If the finding for any requirement or sub-requirement is “Not in Place”, select “Not in Place” for the high-level requirement.
2. If the finding for any requirement or sub-requirement is “N/A” and all other requirements are “In Place”, select “In Place” for the high-level requirement..
3. If the finding for any requirement or sub-requirement is “In Place w/CCW” and all other requirements are “In Place”, select “In Place w/CCW” for the high-level requirement.
4. If the findings include one or more requirements or sub-requirements as “N/A”, and one or more as “In Place w/CCW”, and all other requirements are “In Place”, select “In Place w/CCW” for the high-level requirement.
5. If all requirements and sub-requirements are identified as “In Place”, select “In Place” for the high-level requirement.

Summary of Findings

		<i>In Place per PCI DSS</i>		<i>In Place</i>	<i>In Place w/CCW</i>	<i>N/A</i>	<i>Not in Place</i>
Part 1: Baseline Security Requirements							
P1-1	Maintain security policies for all personnel	☒	OR	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P1-2	Secure network connectivity			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P1-3	Develop and maintain secure systems			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P1-4	Vulnerability management			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P1-5	Manage access			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P1-6	Physical security			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P1-7	Incident response preparedness			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Part 2: 3DS Security Requirements							
P2-1	Validate scope			☒	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P2-2	Security governance			☒	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P2-3	Protect 3DS systems and applications			☒	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P2-4	Secure logical access to 3DS systems			☒	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P2-5	Protect 3DS data			☒	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P2-6	Cryptography and key management			☒	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
P2-7	Physically secure 3DS systems			☒	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite PCI 3DS assessment, which is documented in an accompanying 3DS Report on Compliance (ROC).

The assessment documented in this attestation and in the 3DS ROC was completed on:	18.02.2023	
Was PCI DSS used to meet PCI 3DS Part 1: Baseline Security Requirements?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Have compensating controls been used to meet any PCI 3DS requirement?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any PCI 3DS requirements identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any PCI 3DS requirements unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI 3DS Validation

This AOC is based on results noted in the 3DS ROC dated **18.02.2023**.

Based on the results documented in the 3DS ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (**check one**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI 3DS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>N&TS GROUP Networks & Transactional Systems Group S.p.A.</i> has demonstrated full compliance with the PCI 3DS Core Security Standard.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI 3DS ROC are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (<i>3DS Entity Company Name</i>) has not demonstrated full compliance with the PCI 3DS Core Security Standard.</p> <p>Target Date for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the applicable payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more requirements are marked “Not in Place” due to a legal restriction that prevents the requirement from being met. This option requires additional review from the applicable payment brand(s).</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The 3DS ROC was completed according to the PCI 3DS Core Security Standard, Version 1.0, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced 3DS ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input checked="" type="checkbox"/>	I have read the PCI 3DS Core Security Standard and I recognize that I must maintain compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI 3DS requirements that apply.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Qualys Inc.</i>

Part 3b. 3DS Entity Attestation

<i>Signature of 3DS Entity Executive Officer</i> ↑	<i>Date:</i> 18.02.2023
<i>3DS Entity Executive Officer Name:</i> Stefania Federici	<i>Title:</i> Chief Financial Officer

Part 3c. 3DS Assessor Acknowledgement

<i>Signature of Duly Authorized Officer of 3DS Assessor Company</i> ↑	<i>Date:</i> 18.02.2023
<i>Duly Authorized Officer Name:</i> Branimir Pacar	<i>Title:</i> Principal Consultant
<i>3DS Assessor Company:</i> Dot.Bit d.o.o.	

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI 3DS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI 3DS Requirement	Compliant to PCI 3DS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)	
	YES	NO		
P1	Maintain security policies for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Secure network connectivity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Develop and maintain secure systems	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Vulnerability management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Manage access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Physical security	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Incident response preparedness	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
P2	Validate scope	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Security governance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Protect 3DS systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Secure logical access to 3DS systems	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Protect 3DS data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Cryptography and key management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Physically secure 3DS systems	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

