

CONFORMITY ASSESSMENT REPORT

Meeting requirements for qualified trust service providers, issuing of qualified certificates for electronic signatures, qualified certificates for electronic seals and qualified time stamps in Regulation (EU) No. 910/2014 of the European Parliament and the Council.

Certification audit – 2nd level		X	
Performed by an accredited conformity assessment body (CAB):		Electrotechnical Testing Institute Pod Lisem 129 171 02 Prague 8 – Troja Czech republic Identification number: 00001481 VAT: CZ00001481 Phone: (+420) 266 104 111 Electronic address: epodatelna@ezu.cz	
CAB is certification body No. 3018 accredited by national accreditation body (NAB):		Czech Accreditation Institute Olšanská 54/3, 130 00 Prague 3, Czech Republic Identification number: 25677675 Electronic address: mail@cai.cz	
Link to the accreditation certificate issued by the NAB:		http://ezu.cz/wp-content/uploads/2017/03/OA_COV_42_2017_EN.pdf http://ezu.cz/wp-content/uploads/2017/03/P1_COV_42_2017_EN.pdf	
AUDITING TEAM:			
Lead auditor:	Roman Csirik	2nd auditor:	
3rd auditor:		4th auditor:	
Technical expert:	Pavel Vondruška	Trainee auditor:	

Registered name and address (registered office) of the assessed organization:	Byte Computer S.A. 98 Kallirois st 11741 Athens Greece
---	---

List of the third parties entrusted by TSP to perform all or parts of its processes supporting the provision of its qualified trust services:	N/A
---	-----

AUDIT DATE:	20/06/2017-23/06/2017
A trust service to which the assessment applies:	1.The issue of qualified certificates for electronic signatures 2.The issue of qualified certificates for electronic seals 4.The issue of qualified electronic time stamps
The extent of audited statutory requirements:	Regulation (EU) No. 910/2014 of the European Parliament and the Council, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC: Article 5, 13, 15, 19, 24, 28, 38, 42
Examined standards, specifications available in public and regulatory requirements:	Regulation (EU) No. 910/2014 of the EP and the Council ETSI EN 319 401 v2.1.1 ETSI EN 319 411-1 v1.1.1 ETSI EN 319 411-2 v2.1.1 ETSI EN 319 401 v2.1.1 ETSI EN 319 411-1 v1.1.1 ETSI EN 319 411-2 v2.1.1 ETSI EN 319 412-1 V1.1.1 ETSI EN 319 412-2 V2.1.1 ETSI EN 319 412-3 V1.1.1 ETSI EN 319 412-4 V1.1.1 ETSI EN 319 412-5 V2.1.1 ETSI EN 319 421 V1.1.1 ETSI EN 319 422 V1.1.1 ETSI TS 119 101 V1.1.1 CEN/TS 419261.

Organization's top management:	Spyridogeorgis Vyzantios President & CEO
Name and position of the employee responsible for the service:	Spyridogeorgis Vyzantios President & CEO
Name and position of the employee responsible for the coordination of preparation and contact with the certification body:	Christos Anifantis IT Consultant
The number of employees affecting the provision of the above-identified trust service:	10

The description of the organization's organizational structure:	<i>Byte Company Profile</i> http://www.byte.gr/en/ http://www.byte.gr/company/who-we-are-en/
---	---

<p>List of public and TSP internal documents that have been the subject matter of the audit:</p>	<p>BYTE Work eIDAS\CP\ BYTE nonQC General Services CA CP_1.004_en BYTE nonQC Services CA CP_1.004_en BYTE QC ePrescription CA CP_1.004_en BYTE QC General CA CP_1.004_en BYTE Root_CP_1.005_en</p> <p>BYTE Work eIDAS\CPS\ BYTE nonQC General Services CA CPS_1.004_en BYTE nonQC Services CA CPS_1.004_en BYTE QC ePrescription CA CPS_1.004_en BYTE QC General CA CPS_1.004_en BYTE Root_CPS_1.005_en</p> <p>BYTE Work eIDAS\PDS\ BYTE_ePrescriptionPDS_1.001_en BYTE_GeneralPDS_1.001_en</p> <p>Reviwed other Documents BYTE Company brief presentation</p> <p>BYTE_TC DocumentationTrust Center - PKI Software & Procedures</p> <p>BYTE_TC Infrastructure Main Data Center _DRS_Test BYTE_TC Infrastructure Physical Security etc</p> <p>BYTE_TC Application Form_Sales_Order & Authorization BYTE_TC PKI_Procedural Controls Personnell Working Groups BYTE_TC Subscriber_Agreement(SA) Termination Agreement MULTICERT BYTE BYTE_TC Risk Assesment-2 BYTE_TC SECURITY INCIDENTS HANDLING-TC BYTE_TC Penetration Test BYTE Termination and Changes of Services Plan</p>										
<p>Time spent on the audit (in total): including time spent</p> <ul style="list-style-type: none"> - with examining the documentation - with assessing the performance of risk analysis - during the audit on-site - with preparing the audit report 	<table border="1"> <tr> <td style="text-align: right;">81</td> <td>hours</td> </tr> <tr> <td style="text-align: right;">15</td> <td>hours</td> </tr> <tr> <td style="text-align: right;">6</td> <td>hours</td> </tr> <tr> <td style="text-align: right;">40</td> <td>hours</td> </tr> <tr> <td style="text-align: right;">20</td> <td>hours</td> </tr> </table>	81	hours	15	hours	6	hours	40	hours	20	hours
81	hours										
15	hours										
6	hours										
40	hours										
20	hours										

Audit methodologies used:

- personal interview on-site
- examining documentation off-site
- sampling on examining records

Comment: Variations that have not been discovered during the audit can exist due to the fact that the audit was performed based on sampling objective evidence. The findings and conclusions of the certification body are without prejudice to the organization's responsibility for ensuring compliance and permanent meeting of the applicable requirements of standards, acts, regulations and agreements.

In addition, the audit plan specifies objectives and the subject matter of the audit (e. g. organization units in individual localities, activities, processes, etc.).

Risk identification and assessment

Document:		
Element to be assessed	Auditor's opinion	Evaluation
Risk identification	TC-RISK ASSESMENT V2	OK
Assessment of importance	TC-RISK ASSESMENT V2	OK
Links to policy	There is a linkage	OK
Links to measures	There is a linkage	OK

Risks identified in the first level of the certification audit

Article/paragraph of the Regulation (process)	Risks	Manner of settlement

Meeting requirements for qualified trust service providers, issuing of qualified certificates for electronic signatures, qualified certificates for electronic seals and qualified time stamps in Regulation (EU) No. 910/2014 of the European Parliament and the Council.

Article/paragraph of the Regulation (process)	Evidence of meeting requirements / Strengths	Opportunities for improvement
Article 5	Data processing and protection	
<p>Par. 1. Processing of personal data</p>	<p>TSP has taken appropriate technical and organizational measures against:</p> <p>(a) unauthorized or unlawful processing of personal data;</p> <p>(b) accidental loss or destruction of, or damage to, personal data.</p> <p>The audit logs are backed up and securely stored for evidential and audit purposes and in order to protect against loss or modification.</p> <p>According: Law 2472/1997 & Law 3471/2006</p> <p>BYTE QC General_CA CPS 9.4.Privacy of Personal Information Subscriber Agreement 7. Personal Data Hellenic Data Protection Authority URL http://www.dpa.gr/portal/page?_pageid=33.43560&_dad=portal&_schema=PORTAL</p>	<p>Upgrade documentation to be compliant with GDPR.</p>
<p>Par. 2. The use of pseudonyms</p>	<p>BYTE QC General_CA CPS 3.1.3. Anonymity or pseudonymous of Subscribers Currently not supported.</p>	
Article 13	Liability for damage and burden of proof	
<p>Par. 1. Liability for damage and burden of proof</p>	<p>TSP obtain appropriate liability insurance according Greek Civil Code's (GCC) <i>article 914</i> (76933837 16/12/2016-16/12/2017 (ETHNIKI Hellenic General Insurance Company)</p>	

	<p>BYTE QC General_CA CPS <i>9.2 Financial Responsibility</i> <i>9.6 Representations & Warranties</i> <i>9.8 Limitations of Liability</i> <i>9.9 Term & Termination</i> <i>9.11 Indemnities</i></p> <p>BYTE QC ePrescription_CA CPS <i>9.2 Financial Responsibility</i> <i>9.6 Representations & Warranties</i> <i>9.8 Limitations of Liability</i> <i>9.9 Term & Termination</i> <i>9.11 Indemnities</i></p>	
<p>Par. 2. Liability for damage upon having duly informed the customer in advance</p>	<p>BYTE QC General_CA CPS <i>9.2 Financial Responsibility</i> <i>9.6 Representations & Warranties</i> <i>9.8 Limitations of Liability</i> <i>9.9 Term & Termination</i> <i>9.11 Indemnities</i></p> <p>BYTE QC ePrescription_CA CPS <i>9.2 Financial Responsibility</i> <i>9.6 Representations & Warranties</i> <i>9.8 Limitations of Liability</i> <i>9.9 Term & Termination</i> <i>9.11 Indemnities</i></p>	
<p>Par. 3. Compliance with national rules</p>	<p>Paragraphs 1 and 2 are applied in accordance with national rules on liability.</p> <p>BYTE QC General_CA CPS <i>9.2 9.2 Financial Responsibility</i> <i>9.6 Representations & Warranties</i> <i>9.8 Limitations of Liability</i> <i>9.9 Term & Termination</i> <i>9.11 Indemnities</i></p> <p>BYTE QC ePrescription_CA CPS <i>9.2 9.2 Financial Responsibility</i> <i>9.6 Representations & Warranties</i> <i>9.8 Limitations of Liability</i> <i>9.9 Term & Termination</i> <i>9.11 Indemnities</i></p>	
<p>Article 15</p>	<p>Accessibility for persons with disabilities</p>	
<p>Accessibility of the services for persons with disabilities</p>	<p>Trust services provided and end-user products used in the provision of those services are accessible for persons with disabilities.</p>	<p>Advanced description options for persons with disabilities.</p>

Article 19	Security requirements applicable to trust service providers	
Par. 1 Security requirements applicable to trust service providers	<p>After the audit, it can be stated that appropriate technical and organizational measures are in place to manage the risks to the security of the provided trust-services.</p> <p>During the audit, the implementation of the documents listed below was reviewed and verified.</p> <p>TC-RISK ASSESMENT V2 BYTE QC General_CA CP BYTE QC ePrescription_CA CP <i>6. Technical Security Controls</i> BYTE QC ePrescription_CA CPS BYTE QC General_CA CPS <i>6. Technical Security Controls</i></p>	Risk assessment needs advanced evaluation.
Par. 2 Notification in case of any breach of security or loss of integrity	<p>Byte_TC Security Incidents Handling</p> <p>Incident reporting framework for eIDAS Article 19 – Enisa</p>	
Article 20	Supervision of qualified trust service providers	
Par. 1. Audit by Conformity Assessment Body	<p>Audited at their own expense at least every 24 months by a conformity assessment body EZU.</p> <p>See: http://ezu.cz/wp-content/uploads/2017/03/OA_COV_42_2017_EN.pdf http://ezu.cz/wp-content/uploads/2017/03/P1_COV_42_2017_EN.pdf</p>	
Par. 2. Audit by Supervisory Body	N/A Up to supervisory body requirement	
Par. 3. Remedy of any failure to fulfill requirements	N/A Up to supervisory body requirement	

Article 24	Requirements for qualified trust service providers	
<p>Par. 1. Verification of identity and specific attributes of the natural or legal person</p>	<p>Qualified TSP when issuing a qualified certificate for a trust service verifies identity by relying on a third party in accordance with national law by the physical presence of the natural person or of an authorised representative of the legal person.</p> <p>BYTE QC General_CA CPS <i>3. Identification and Authentication</i> BYTE QC ePrescription_CA CPS</p>	
<p>Par. 2 (a) Information about changes</p>	<p>BYTE Termination and Changes of Services Plan</p>	<p>More advanced description procedure for announcement of changes</p>
<p>Par. 2 (b) Employees, subcontractors and administrative and management procedures</p>	<p>Qualified TSP employ staff and subcontractors with the required competencies.</p> <p>Byte PKI Working Groups <i>2. Working Group – Trusted Roles</i> <i>3. Personnel Safety Measures & Controls</i> Annual Report to Supervisor Body</p>	
<p>Par. 2 (c) Risk of liability for damage</p>	<p>Qualified TSP obtain appropriate liability insurance, in accordance with national law.</p> <p>BYTE QC General_CA CPS <i>9.2 Financial Responsibility</i> <i>9.6 Representations & Warranties</i> <i>9.8 Limitations of Liability</i> <i>9.9 Term & Termination</i> <i>9.11 Indemnities</i></p> <p>BYTE QC ePrescription_CA CPS <i>9.2 Financial Responsibility</i> <i>9.6 Representations & Warranties</i> <i>9.8 Limitations of Liability</i> <i>9.9 Term & Termination</i> <i>9.11 Indemnities</i></p>	
<p>Par. 2 (d) Information about the conditions regarding the use of the service</p>	<p>Qualified TSP before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that</p>	

	<p>service, including any limitations on its use.</p> <p>BYTE QC General_CA CPS</p> <p><i>9.2 Financial Responsibility</i></p> <p><i>9.6 Representations & Warranties</i></p> <p><i>9.8 Limitations of Liability</i></p> <p><i>9.9 Term & Termination</i></p> <p><i>9.11 Indemnities</i></p> <p>BYTE QC ePrescription_CA CPS</p> <p>BYTE_TC Subscriber_Agreement(SA)</p>	
<p>Par. 2 (e) Use of trustworthy systems and products</p>	<p>Qualified TSP use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.</p> <p>BYTE QC General_CA CPS</p> <p><i>4. Certificate Life-Cycle Operational Requirements</i></p> <p><i>5. Facility, Management, Operational and Physical Controls</i></p> <p><i>6. Technical Security Controls</i></p> <p>BYTE QC ePrescription_CA CPS</p> <p><i>4. Certificate Life-Cycle Operational Requirements</i></p> <p><i>5. Facility, Management, Operational and Physical Controls</i></p> <p><i>6. Technical Security Controls</i></p> <p>ISO 9001:2008</p> <p>ISO 27001:2014</p> <p>BYTE QC ePrescription CA CP</p> <p>BYTE QC General CA CP</p> <p><i>5. Facility, Management, Operational, and Physical Controls</i></p>	
<p>Par. 2 (f) Data storing</p>	<p>Qualified TSP use trustworthy systems to store data provided to it, in a verifiable form so that: (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained, (ii) only authorised persons can make entries and changes to the stored data, (iii) the data can be checked for authenticity</p> <p>BYTE QC General_CA CPS</p> <p><i>5.4 Audit logging procedures</i></p> <p><i>5.5 Record Archival</i></p>	

<p>Par. 2 (g) Measures against forgery and theft of data</p>	<p>Qualified TSP take appropriate measures against forgery and theft of data See: TC Risk Assessment v2</p>	
<p>Par. 2 (h) Recording information concerning data and keeping it accessible</p>	<p>Qualified TSP record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider.</p> <p>BYTE QC General_CA CPS <i>5.4 Audit logging procedures</i> <i>5.5 Record Archival</i></p> <p>BYTE QC ePrescription_CA CPS <i>5.4 Audit logging procedures</i> <i>5.5 Record Archival</i></p>	
<p>Par. 2 (i) Termination plan</p>	<p>TSP has an up-to-date termination plan to ensure continuity of service in accordance with provisions. (in accordance REGULATION_248_71_2002) See: BYTE QC General_CA CPS 5.8 CA termination BYTE QC ePrescription_CA CPS 5.8 CA termination BYTE QC ePrescription CA CP BYTE QC General CA CP REGULATION_248_71_2002</p>	<p>Termination plan to ensure continuity of service in accordance with provisions should be verified by the supervisory body under point (i) of Article 17(4);</p>
<p>Par. 2 (j) Processing of personal data</p>	<p>The TSP Processing of personal data in accordance with Directive 95/46/EC and in a trustworthy manner and in accordance with:</p> <p>BYTE QC General_CA CPS <i>9.4.Privacy of Personal Information</i> Subscriber Agreement <i>7. Personal Data</i> Hellenic Data Protection Authority URL http://www.dpa.gr/portal/page?_pageid=33.43560&_dad=portal&_schema=PORTAL</p>	

Par. 2 (k) Certificate database	Qualified TSP, establish and keep updated a certificate database.	
Par. 3 Revocation of certificates	If a Qualified TSP decides to revoke a certificate then register revocation in its certificate database and publish revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation become effective immediately upon its publication. See: BYTE_TC Subscriber_Agreement(SA) BYTE QC ePrescription CA CP BYTE QC General CA CP <i>4. Certificate Life-cycle Operational Requirements</i> <i>7. Certificate and CRL Profiles</i>	
Par. 4 Providing information about status of issued qualified certificates	Qualified TSP provide to any relying party information on the validity or revocation status of qualified certificates issued by them free of charge and according requirements of this par. 4. BYTE QC General_CA CPS <i>4.9. Certificate Suspension and Revocation</i> <i>7. Certificate and CRL Profiles</i>	
Article 28	Qualified certificates for electronic signatures	
Par. 1. Meeting the requirements laid down in Annex I to the Regulation	Qualified certificates for electronic signatures meet the requirements laid down in Annex I Functional Specifications BYTE QC General_CA CP <i>7. Certificate and CRL Profiles</i> <i>7.1.3 Profile of the Qualified Digital Signature Certificate</i> BYTE QC ePrescription_CA CP <i>7. Certificate and CRL Profiles</i> <i>7.1.3 Profile of the Qualified Digital Signature Certificate</i>	
Par. 3. Specific attributes of qualif. certificates	Qualified certificates for electronic signatures include non-mandatory additional specific attributes. BYTE QC General_CA CP <i>7.1 Certificate Profile</i>	

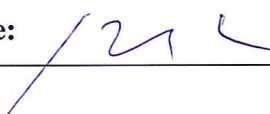
	<p><i>7.1.3 Profile of the Qualified Digital Signature Certificate</i></p> <p>BYTE QC ePrescription_CA CP</p> <p><i>7.1 Certificate Profile</i></p> <p><i>7.1.3 Profile of the Qualified Digital Signature Certificate</i></p>	
<p>Par. 4. Revocation of a qualif. certificate</p>	<p>Qualified certificate for electronic signatures has been revoked after initial activation, it lose its validity from the moment of its revocation, and its status can not in any circumstances be reverted.</p> <p>BYTE QC General_CA CPS</p> <p><i>4.9.Certificate Suspension and Revocation</i></p> <p>BYTE QC ePrescription_CA CPs</p> <p><i>4.9.Certificate Suspension and Revocation</i></p>	
<p>Par. 5. National rules on temporary suspension of qualified certificates</p>	<p>Qualified TSP support temporary suspension for temporary period max. 5 working days.</p> <p>BYTE QC General_CA CPS</p> <p><i>4.9.Certificate Suspension and Revocation</i></p> <p><i>4.9.4 Limited Time Period for Suspension (max 5 working days)</i></p> <p>BYTE QC ePrescription_CA CPs (same as above)</p> <p>No specific guidance given at this time at National level</p>	
Article 38	Qualified certificates for electronic seals	
<p>Par. 1. Meeting the requirements laid down in Annex III to the Regulation</p>	<p>Qualified certificates for electronic seals meet the requirements laid down in Annex III Functional Specifications</p> <p>BYTE QC General_CA CP</p> <p><i>7. Certificate and CRL Profiles</i></p> <p><i>7.1.4 Profile of the Qualified Electronic Seal Certificate</i></p>	
<p>Par. 3. Specific attributes of qualif. certificates</p>	<p>Qualified certificates for electronic signatures include non-mandatory additional specific attributes.</p> <p>BYTE QC General_CA CP</p> <p><i>7.1 Certificate Profile</i></p>	

<p>Par. 4. Revocation of a qualif. certificate</p>	<p>Qualified certificate for electronic sealss has been revoked after initial activation, it lose its validity from the moment of its revocation, and its status can not in any circumstances be reverted. BYTE QC General_CA CPS <i>4.9.Certificate Suspension and Revocation</i></p>	
<p>Par. 5. National rules on temporary suspension of qualified certificates</p>	<p>Qualified TSP support temporary suspension. BYTE QC General_CA CPS <i>4.9.Certificate Suspension and Revocation</i> <i>No specific guidance given at this time at National level from supervisor body</i></p>	
<p>Article 42</p>	<p>Requirements for qualified electronic time stamps</p>	
<p>Par. 1. (a) Date and time</p>	<p>Timestamp Services & Policies <i>2. Physical Infrastructure</i> <i>3. Logical Infrastructure</i></p>	
<p>Par. 1. (b) Accurate time source</p>	<p>Timestamp Services & Policies <i>2. Physical Infrastructure</i> <i>3. Logical Infrastructure</i></p>	
<p>Par. 1. (c) Identification of a time stamp</p>	<p>Timestamp Services & Policies <i>2. Physical Infrastructure</i> <i>3. Logical Infrastructure</i></p>	

Total Summary

A – excellent situation, B – decent situation, C – deficiencies, D – non-compliance)

Regulation (EU) No. 910/2014 of the EP and the Council	A	B	C	D	Comments
Article 5 Data processing and protection		X			
Article 13 Liability and burden of proof		X			
Article 15 Accessibility for persons with disabilities		X			
Article 19 Security requirements applicable to trust service providers		X			
Article 24 Requirements for qualified trust service providers		X			
Article 28 Qualified certificates for electronic signatures	X				
Article 38 Qualified certificates for electronic seals	X				
Article 42 Requirements for qualified electronic time stamps	X				

Non-compliance:		
Deficiencies:		
Proposed term for Surveillance audit:	From 18 to 22 June 2018	
The latest date for Recertification audit:	Before the certificates expire.	
Conclusion:		
<p>The objectives of the audit have been met.</p> <p>Based on the audit, the auditing team states compliance <i>non-compliance</i> with the above requirements of Regulation (EU) No. 910/2014 of the European Parliament and the Council.</p> <p>The certification body will examine all audit materials independently prior to its decision.</p>		
Declaration:		
<p>I/we confirm that to the best of my knowledge and belief, I/we have no personal or other impairments that will prevent me/us from objectively planning, conducting, reporting or otherwise participating and reaching independent conclusions in Audit Assignment for Byte Computer S.A., according to the above referenced regulations.</p> <p>Should I/we become aware of any changes in my circumstances, I/we will promptly notify the Auditee, the Supervisory Authority, the management of Conformity Assessment Body and the National Accreditation Body.</p>		
Date: 27 June 2017		
Lead auditor: Roman Csirik	Signature: 	

EVALUATION BY THE CERTIFICATION BODY

The result is checked off in the relevant box.

	DEGREE OF CRITICS	RECOMMENDED MEASURE	
1	No cases of non-compliance, a limited number of deficiencies.	To award the Declaration of Conformity.	<input checked="" type="checkbox"/>
2	A limited number of material cases of non-compliance or a higher number of deficiencies.	To award the Declaration of Conformity after measures to remove the cases of non-compliance have been submitted.	<input type="checkbox"/>
3	A higher number of material cases of non-compliance. Significant endangering the compliance with the Regulation.	The organization has to take more extensive corrective measures. New assessment.	<input type="checkbox"/>
4	A great number of material cases of non-compliance – non-compliance with the Regulation.	The organization has not yet been eligible for certification and service re-engineering and new verification are required. Not to award the Declaration of Conformity.	<input type="checkbox"/>

CONCLUSION

The Declaration of Conformity **will be** ~~will not be~~ awarded.

Comments:

Product Manager for eIDAS

Date: 27.6.2017


Michal Hager

Annexes to the Report: Audit plan, appointment of the auditing team.

Distribution list for the audit report: 1 original – certified organization
1 copy – EZÚ

Opinion of the audited organization’s representative:

on the result of the Audit Report	I agree	I do not agree
with the procedure taken by the auditing team	I agree	I do not agree

Check off your opinion in the table please

Comments:

Date:

Signature of the organization’s representative:

In case that we do not receive your opinion on the Audit Report and on the procedure of the auditing team within 15 days as of the delivery, we consider that your opinion is positive.