



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Bundesamt für Landestopografie swisstopo

NGDI-Zwischenbericht / NGDI-Schlussbericht

Dieses Projekt ist durch den Bund mit zweckgebundenen NGDI-Finanzmitteln unterstützt worden.
Ce projet a été soutenu par la Confédération avec des moyens dédiés à l'INDG.

Maximal 6 Seiten!

Dokumenten- und Versandinformation

Verfasser ! Auteur

| Verfasser (Name, Vorname) Auteur (nom, prénom) | Firma / Organisation entreprise / organisation | Datum date | Bemerkungen commentaires |
|---|---|---------------|-----------------------------|
| Kuhn Matthias | OPENGIS.ch | 25.6.2021 | |

Review durch Projektkoordinator ! xxxxxxxxxxxxxx

| Datum date | Bemerkungen commentaires |
|---------------|--|
| 29.06.2021 | Die Stammdaten des Projektes müssen angepasst werden. Der Bericht muss in Französisch oder Deutsch verfasst sein. Der Bericht muss sich auf die technische Dokumentation beziehen. |
| 26.07.2021 | Keine |

Versand an Steuerungsorgan ! xxxxxxxxxxxxxx

Die Termine für den Versand an das Steuerungsorgan sind dem Vertrag zu entnehmen.
Les dates d'envoi à l'organe de pilotage sont précisées dans le contrat.

| Absender (Mailadresse des Antragsstellers) xxxxxxxxxxxxxxxxxxxx | Adressat xxxxxxxxxxxxxxxxxxxx | Cc (Mailadresse des Projektkoordinators) xxxxxxxxxxxxxxxxxxxx | Datum date |
|--|----------------------------------|--|---------------|
| matthias@opengis.ch | ngdi@kkgeo.ch | Pasquale.DiDonato@swisstopo.ch | 26.07.21 |

Stammdaten des Projektes ! xxxxxxxxxxxxxxxxxxxxxxxx

| | |
|--|--|
| Nr. NGDI N° INDG | 20-56 |
| Titel Titre | Sécurisation double facteur pour l'accès aux géodonnées |
| Antragsteller (Organisation) Demandeur (organisation) | OPENGIS.ch GmbH |
| Antragsteller (verantwortliche Person) Demandeur (personne responsable) | Matthias Kuhn |
| Projektpartner (Organisation) Partenaire de projet (organisation) | Ville d'Yverdon-les-bains |
| Projektleiter Responsable de projet | Olivier Monod |
| Projektkoordinator (PROK) Coordinateur de projet (PROK) | Pasquale Di Donato |
| Vertragssumme inkl. MWST | 16'155.00 |

| | |
|--------------------------------|-----------|
| Montant contractuel avec TVA | |
| Vertragsende Fin du contrat | 30.9.2021 |

Inhaltsverzeichnis

| | |
|---|---|
| 1 | 2 |
| 2 | 3 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 5 |
| 7 | 5 |

1 Management Summary

| Bereich | Status | Bemerkung |
|---|--------|-----------|
| Gesamtbeurteilung | | |
| Termine | | |
| Kosten | | |
| Ergebnisse | | |
| Projektziele | | |
| NGDI-Ziele | | |
| Legende: Gelb: (un)genügend / problematisch / ev. Massnahmen nötig Rot: schlecht / Massnahmen nötig Grün: gut / auf Kurs, | | |

| |
|------------------------------|
| Weitere Informationen |
| ... |

2 Wesentliche Kennzahlen

| | |
|---|------------|
| Bisher gestellte Rechnungen + geleistete, aber noch nicht in Rechnung gestellte Arbeiten [in CHF, inkl. MWST] (1) | CHF15416.1 |
| Vertragssumme [in CHF, inkl. MWST] (2) | CHF16155 |
| Offenes Budget CHF = (2) - (1) (3) | CHF738.9 |
| Offenes Budget in % = (3) / (2) | 4.5% |
| Geschätzter Arbeitsstand [in %] | 100% |
| Bemerkung | |

3 Vorgehen

Les logiciels OpenSource QGIS et QField sont aujourd'hui largement répandus au sein des administrations publiques à tous les niveaux d'organisation. Dans une optique d'intégration centralisée des géodonnées publiques, il est primordial que les logiciels SIG supportent l'authentification à double facteur afin de garantir la sécurité de ces données. Cette sécurisation apparaît comme une condition-cadre de toute intégration centralisée de géodonnées.

Objectifs initiaux

Afin de réaliser une authentification à double facteur pour QField sur le site, l'idée initiale était de mettre en œuvre un élément d'interface utilisateur spécifique pour QField ainsi que pour QGIS afin de permettre la connexion avec un deuxième facteur sous la forme d'un "time-based one time password" (TOTP) au portail web basé sur GeoMapFish. Le portail web met déjà en œuvre cette forme d'authentification via un formulaire de connexion personnalisé.

Au cours de l'examen initial du système, il s'est avéré que celui-ci est basé sur un protocole d'authentification personnalisé. Afin de maximiser la réutilisabilité de ce développement et d'éviter de s'enfermer dans un seul système, le champ d'application a été ajusté pour une approche générique.

OAuth2

OAuth2 est un protocole standard de l'industrie pour l'autorisation. Il transmet l'authentification à un site Web dédié et accorde l'autorisation aux applications par le biais d'un flux de codes d'autorisation. Grâce à cela, les applications clientes (QField ou QGIS) peuvent obtenir une autorisation pour les services tout en ignorant les détails de mise en œuvre de l'authentification.

Afin de réaliser ceci

- Les fournisseurs d'authentification de QGIS ont été remaniés pour séparer les composants spécifiques aux interfaces graphiques (applications de bureau) des composants de base (logiques).

- Les composants de base (logiques) ont été intégrés dans QField.
- QGIS a été étendu pour prendre en charge l'exportation des configurations d'authentification au format XML.
- QField a été étendu pour supporter l'importation des configurations d'authentification en XML.

Résultats

Ce projet, d'ampleur limitée, met en évidence la nécessité pour les professionnels de la géoinformations de se conformer autant que faire se peut, aux standards en matière de technologies web. Parmi celles-ci un élément central est le support des protocoles d'authentification permettant une sécurisation suffisante afin de rendre possible les échanges données de nature sensible. Ce projet apporte une contribution importante à un potentiel décloisonnement des géodonnées, qui trop souvent, sont isolées les unes des autres. L'approche est ici centrée sur les webservices qui paraissent plus à même de répondre aux challenges futurs que des formats de fichiers d'échanges, aussi normés soient-ils.

Au terme de ce projet il est possible, à l'aide de 3 solutions entièrement Open Source (QGIS, QField & Geomapfish) d'échanger des géodonnées sensibles en garantissant une sécurité suffisante en matière d'authentification.

Documentation

Une documentation a été rédigée afin de faciliter la configuration par les utilisateurs:

<https://qfield.org/docs/prepare/authentication.html>

Informations techniques

La liste suivante de demandes de retrait contient les détails techniques et les discussions connexes pour les éléments clés de cette mise en œuvre.

- <https://github.com/opengisch/QField/pull/1907>
- <https://github.com/qgis/QGIS/pull/43866>
- <https://github.com/qgis/QGIS/pull/43262>
- <https://github.com/qgis/QGIS/pull/43193>

4 Resultate

- Les méthodes d'authentification de QGIS ont été remaniées pour séparer les composants spécifiques aux interfaces graphiques (applications desktop) des composants de base (logiques).
- Les composants de base (logiques) ont été intégrés dans QField.
- QGIS a été adapté pour prendre en charge l'exportation des configurations

- d'authentification au format XML.
- QField a été adapté pour prendre en charge l'importation des configurations d'authentification au format XML.
- Une documentation sur l'utilisation d'OAuth2 avec QField a été rédigée.
<https://qfield.org/docs/prepare/authentication.html>
- Les bibliothèques d'authentification de QGIS peuvent maintenant être compilées en tant que bibliothèques statiques (exigence pour les expédier sur iOS)

5 Meilensteine

| Meilenstein (Beschreibung) | Datum | |
|-------------------------------|-----------|-----------|
| | geplant | erreicht |
| Livraison finale | 30.6.2021 | 30.6.2021 |

6 Risiken / Probleme

| Risiko / Problem | Vorschlag / Empfehlung für Massnahme/n zur Risikominderung / Problemlösung |
|------------------|--|
| - | - |

7 Ausblick / Weiteres Vorgehen

Le déploiement dans l'environnement de production chez le client n'a pas encore eu lieu. Il est prévu pour plus tard cette année.

La documentation de GeoMapFish a fait l'objet d'une discussion et il est souhaitable d'y ajouter du matériel supplémentaire sur la manière de mettre en œuvre avec succès QField avec l'authentification à deux facteurs pour ce cas d'utilisation spécifique et cette combinaison de technologies.