Registry collaboration on detecting malicious registrations

Thijs van den Hout (.nl), Ronald Geens (.be)

ICANN/ccNSO DASC

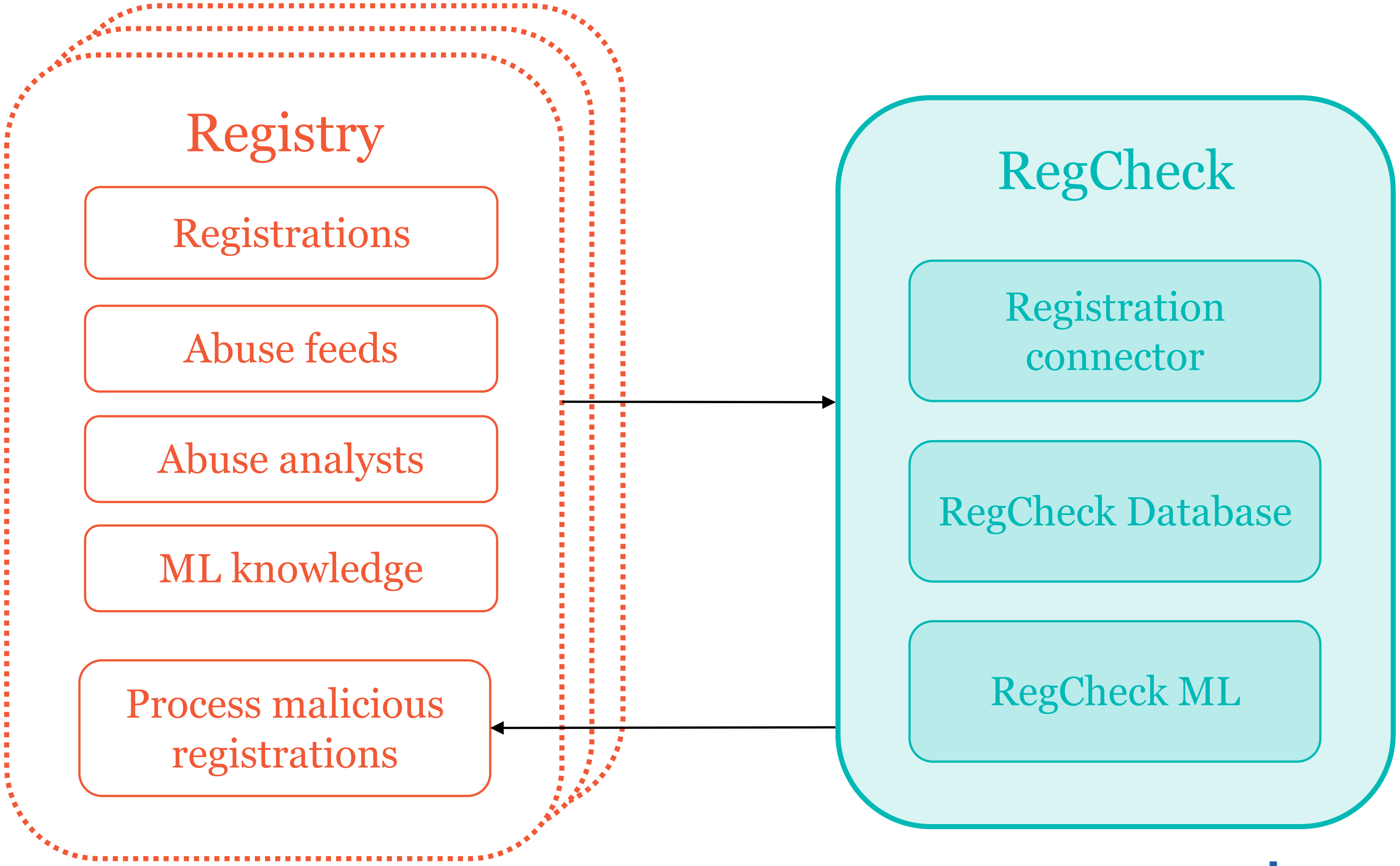
2023-10-25

dnsbelgium SIDN LABS

Agenda

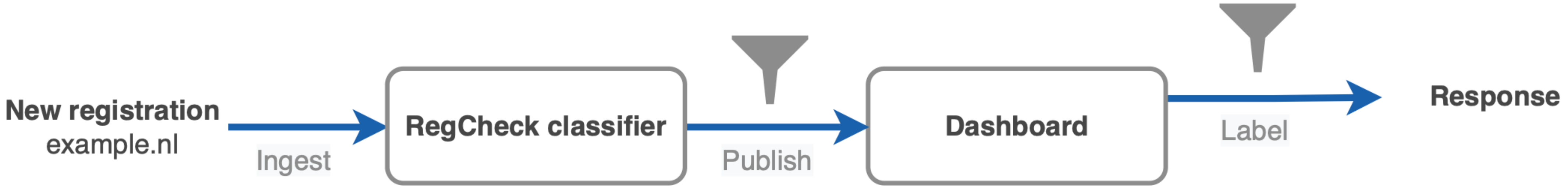
- RegCheck: ML-based detection of malicious registrations
- .nl approach
- .be approach
- Registry collaboration
- Lessons learned

RegCheck (as seen on TechDay)

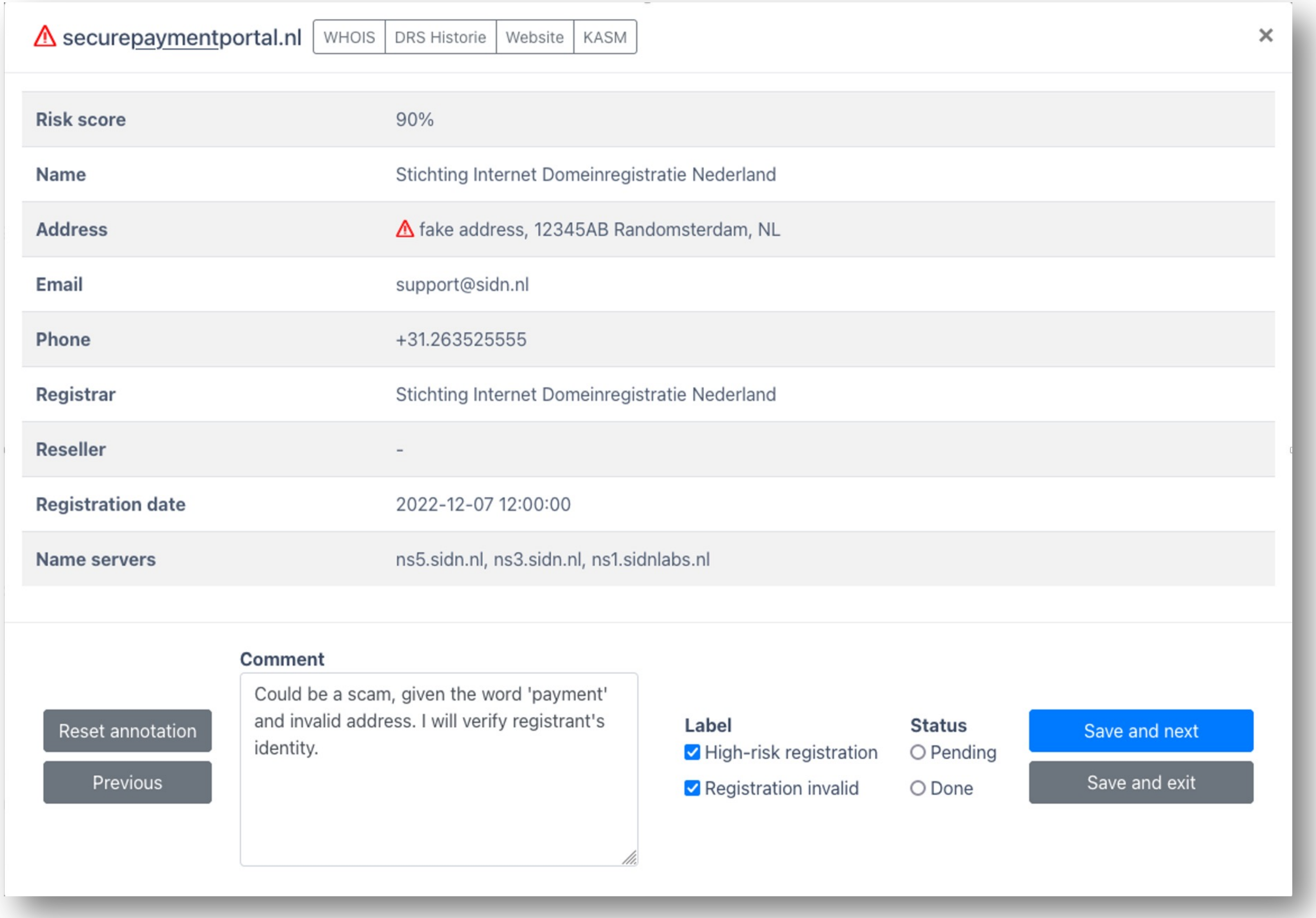


.nl approach

- All new registrations enter the zonefile
- RegCheck retrospectively computes risk scores
- Results published on support dashboard
- Start ID verification for suspicious registrations
- Prioritise precision over recall



.nl approach



⚠ securepaymentportal.nl

Risk score	90%
Name	Stichting Internet Domeinregistratie Nederland
Address	⚠ fake address, 12345AB Randomsterdam, NL
Email	support@sidn.nl
Phone	+31.263525555
Registrar	Stichting Internet Domeinregistratie Nederland
Reseller	-
Registration date	2022-12-07 12:00:00
Name servers	ns5.sidn.nl, ns3.sidn.nl, ns1.sidnlabs.nl

Comment: Could be a scam, given the word 'payment' and invalid address. I will verify registrant's identity.

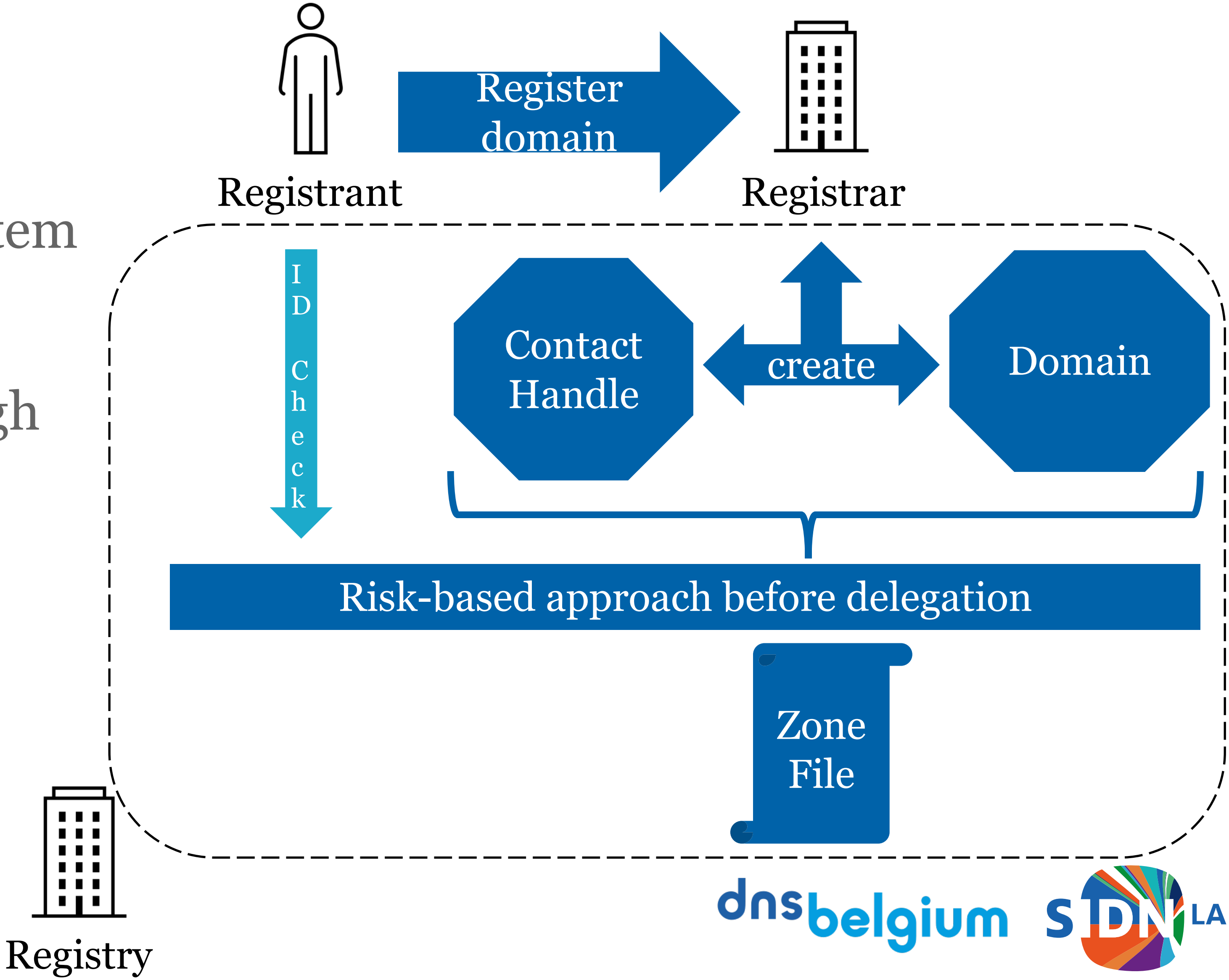
Label: ☑ High-risk registration ☑ Registration invalid

Status: ○ Pending ○ Done

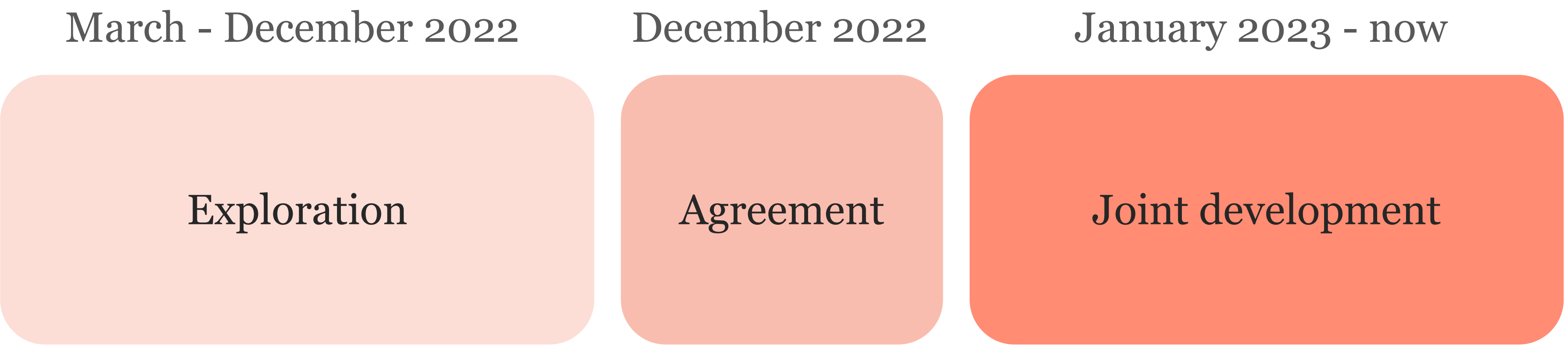
- 44% of ID verifications started with RegCheck
- <5% of registrants respond to request
- Quantitative evaluation is difficult

.be approach

- Rule based system
- Deferred delegation
- Experimental ML based system
- Moving to RegCheck
- Optimizing differently though
  - Recall over precision
  - Additional input data



Collaboration phases



March - December 2022

Exploration

December 2022

Agreement

January 2023 - now

Joint development

Benefits of collaboration

- Improved reputation scoring
- Validation of geographical features (e.g., city, timezone)
- Added TF-IDF-based features on registrant fields
- Handle high-cardinality n-gram features
- Discussion about design and policy choices

Lessons learned

- Sharing experiences with / different views on abuse is valuable
- Collaboration works, even with diverging policies
- Collaboration inspires innovation
- More people = more opinions